Chapter 3

Point-to-Point Protocol (PPP)

Introduction

This chapter describes the main features of the Point-to-Point Protocol (PPP), support for the Point-to-Point Protocol on the router, and how to configure network interfaces on the router to use the Point-to-Point Protocol.

The Point-to-Point Protocol was developed by the Internet Engineering Task Force (IETF) as a means of transmitting data for more than one network protocol over the same point-to-point serial link in a standard, vendor-independent way. The Point-to-Point Protocol provides mechanisms for transmitting data over synchronous connections, ISDN, ACC and L2TP calls, and groups of TDM slots.

The Point-to-Point Protocol

The Point-to-Point Protocol consists of three main components:

- A method for encapsulating datagrams over serial links.
- A Link Control Protocol (LCP) for establishing, configuring, and testing the data-link connection.
- A family of Network Control Protocols (NCPs) for establishing and configuring different network-layer protocols.

The mechanism that PPP uses to carry network traffic is to open a link with a short exchange of packets. Once the link is open, network traffic is carried with very little overhead. Frames are sent as unnumbered information frames, so no data link acknowledgement is required and no retransmissions are carried out. Once the link is established, PPP acts as a straight data pipe for protocols.

Encapsulation

The Point-to-Point Protocol is, at the lowest level, an example of the HDLC protocol, with the following features:

- Data comes in frames, delimited by special characters called flags.
- When a frame is not being sent, the sender transmits flags continually. This means that there is constant activity on any synchronous line that is running properly.
- The first four bytes of a PPP frame comprise a 1 octet address field which is always set to 0xFF, a 1 octet control field which is always set to 0x03 (“unnumbered information”) and a 2-octet protocol field.
- The data that follows the address and control fields is interpreted by the device receiving the frame depending on the encapsulation type.

A Link Control Protocol (LCP) exists to bring up the PPP link before any other protocols can begin transmission. Each protocol carried over PPP has an associated Network Control Protocol (NCP) that negotiates options for the protocol and brings up the link for that protocol (Table 3-1 on page 3-4).

Table 3-1: Supported Network protocols and Network Control Protocols for the Point-to-Point Protocol.

Protocol	PPP Type (hexadecimal)
LCP	0xC021
IP	0x0021
IPCP	0x8021
TCP/IP Comp	0x002D
TCP/IP Uncomp	0x002F
IPX	0x002B
IPXCP	0x802B
DECnet	0x0027
DECnetCP	0x8027
AppleTalk	0x0029
ATCP	0x8029
Multilink	0x003D
Individual Link Compression	0x00FB
ILCCP	0x80FB
Compression	0x00FD
CCP	0x80FD
Encryption	0x0053
ECP	0x8053
Bridging	0x0031
Bridge Spanning Tree	0x0201
BCP	0x8031
Link Quality Report	0xC025
Password Authentication Protocol (PAP)	0xC023
Challenge-Handshake Authentication Protocol (CHAP)	0xC223

The TCP/IP Comp and TCP/IP Uncomp protocols provide direct support for Van Jacobson's header compression. For more information on Van Jacobson's header compression see Chapter 8, Internet Protocol (IP).

Control Protocols

Control protocols are protocols run by PPP between the two stations at either end of a link to allow the link to be used to carry a particular type of traffic. The Link Control Protocol (LCP) must run before any other control protocol in order to allow the link to be used at all.

The local and remote stations negotiate the configuration options to be used on the link. A *configure request packet* is sent first containing configuration options. The remote station responds with a packet confirming that the options are okay, suggesting different options or rejecting the options. This exchange takes place in both directions and when a station has sent and received an acknowledge packet the link is declared open.

Once the link has been opened by the LCP, any authentication that is required is performed. When authentication has been completed successfully, or if no authentication is required, then a Network Control Protocol (NCP) is run for each network layer protocol using the link. The NCPs operate in a similar way to the LCP, negotiating configuration options specific to the network layer protocol. No NCPs can use the PPP link until the LCP has opened the link, and no data packets can be exchanged unless the appropriate NCP is open.

Control protocols consist of states, events and packets. Events cause the state of a link to change (Table 3-2 on page 3-5). Two important events are OPEN and CLOSE. They can be caused either by a management command or internally, for example, when the router powers up. An OPEN event causes the control protocol to try to establish a link and a CLOSE event terminates a link. Other events are the hardware becoming available (UP) or unavailable (DOWN), timeouts, and the arrival of packets.

Table 3-2: States for control protocols of the Point-to-Point Protocol.

State	Meaning
INITIAL	Startup state; no OPEN event has occurred and the hardware is DOWN.
STARTING	An OPEN event has occurred and the hardware is DOWN.
CLOSED	The hardware is UP and no OPEN event has occurred.
STOPPED	The hardware is UP and a DOWN or TIMEOUT event has occurred.
CLOSING	The link has been UP and a CLOSE event has occurred; trying to close link.
STOPPING	The link has been OPEN and the remote station is trying to CLOSE the link.
REQ SENT	A configure request has been sent; waiting for a reply.
ACK RCVD	A configure request has been sent, and an acknowledge received.
ACK SENT	A configure request has been received, and an acknowledge sent.
OPENED	An acknowledge has been sent and received.

The state of a PPP link (LCP) and the NCPs running on that link can be displayed with the command:

```
SHOW PPP
```

LCP Options

The LCP will attempt to negotiate the following options:

- Maximum Receive Unit (MRU).
- Endpoint Discriminator.
- Link Discriminator, as defined in RFC 2125.
- Authentication Protocol.
- Link Quality Reporting (LQR).
- Magic Number.
- Asynchronous Control Character Map (ACCM).
- Maximum Received Reconstructed Unit (MRRU).

All other options are set to the default values specified in the relevant RFC.

Endpoint Discriminator Option

The Endpoint Discriminator Option is defined in RFC 1990 and is required for PPP to form multilink bundles from dynamic PPP calls. The Endpoint Discriminator provides a mechanism for identifying the physical location of the peer at the remote end of a PPP link. When two or more dynamic PPP calls are made from the same peer, with the same authentication information, they can be bundled together to form a multilink interface if they have the same Endpoint Discriminator. The router uses its MAC address to identify itself.

If an Endpoint Discriminator is received during LCP negotiation on a newly activated link in a static PPP interface with more than one link, and that Endpoint Discriminator value is different from the Endpoint Discriminators received during negotiation on the other active links in the interface, then the new link with the invalid Endpoint Discriminator will be deactivated.

Link Discriminator Option

The Link Discriminator Option is defined in RFC 2125 and is required for the operation of BAP. During LCP negotiation it is used to declare a unique identifier for the link over which the negotiation is occurring. This unique identifier is used by BAP to differentiate the various links in a multilink bundle.

Link Quality Management

Link quality management is used to determine the quality of a PPP link. A *Link Quality Report* (LQR) packet is transmitted down the link by the router at regular intervals. This LQR packet contains information which is used to determine how many packets are being lost on the link. The interval between transmissions of LQR packets is determined by the LQR timer value obtained from the peer during the negotiation of the LQR LCP option. This timer value, which defines how often the peer expects to see an LQR packet, is configured at the peer using the commands:

```
CREATE PPP=ppp-interface OVER=physical-interface LQR=time
SET PPP=ppp-interface OVER=physical-interface LQR=time
```

If an LQR packet is not seen by the peer within twice the configured timer value the link is deemed to have failed and is reset.

Each LQR packet also contains the magic number determined during the LCP negotiation process. If the magic number in an incoming LQR packet is the same as the local magic number then the link is deemed to be in loopback mode and is reset.

Multilink PPP

PPP provides a mechanism for combining a number of PPP links into a single bundle of links, whose bandwidth is the sum of the bandwidths of the individual links. This mechanism is known as multilink PPP (MP) and is described in RFC 1990.

When a packet is transmitted over a multilink bundle it is encapsulated by a multilink header which includes information to allow the packets sent over the links in the bundle to be sequenced. This gives the multilink bundle the same properties as a single PPP link. This encapsulation also includes information

that allows large packets to be fragmented, spreading the data across a number of links and giving better packet throughput in some circumstances.

When a packet is about to be transmitted across a PPP multilink bundle, a decision is made as to which link to use to transmit the packet. If all link speeds in the multilink bundle are the same, and packets are being transmitted at a rate so that each packet has been transmitted before the next packet arrives for transmission, a round-robin scheme is used to choose between links. If there is a choice between two or more equally desirable links the packet will be sent on the link that was least recently used. Rotating traffic in this way prevents links from remaining idle for long periods of time and reduces the number of null fragments that must be transmitted during idle periods.

Both static and dynamic PPP interfaces can be multilinked. The Endpoint Discriminator LCP option ("*Endpoint Discriminator Option*" on page 3-6) enables a single dynamic PPP interface to accept and bundle more than one call. If two or more dynamic PPP calls are made from the same peer with the same authentication information, they will be bundled together to form a multilink interface.

Van Jacobson's TCP/IP header compression should not be enabled on a multilink PPP interface.

Bandwidth Allocation Protocol

The Bandwidth Allocation Protocol (BAP), defined in RFC 2125, provides a mechanism for two PPP peers to manage the bandwidth available to the protocols using a multilink PPP bundle by negotiating gracefully to add and remove links from the multilink bundle. The negotiation process allows each peer to choose the algorithm used to determine when to add or remove links in the multilink bundle.

The Bandwidth Allocation Control Protocol (BACP), defined in RFC 2125, is a standard PPP NCP protocol used to negotiate the use of BAP on a multilink PPP interface. BACP is negotiated once per multilink bundle. If BACP is negotiated on any of the links in a multilink bundle, it is opened for all of the links in the bundle. BACP must be successfully negotiated before BAP can be used.

The Favoured Peer Option is the only option defined for BACP and is used to determine which peer is favoured in the event that both peers simultaneously transmit the same BAP request. Each peer negotiates a 4-octet magic number, which is successfully negotiated when the two magic numbers are different. The favoured peer is the peer with the lowest magic number.

After BACP reaches the opened state, either peer can request that another link be added to the bundle by sending a BAP *Call-Request* or *Callback-Request* packet. A *Call-Request* packet is sent if the peer wishes to originate the call for the new link, and a *Callback-Request* packet is sent if the peer wishes its remote peer to originate the call for the new link.

A peer can also request that a link be dropped from the bundle. A BAP *Link-Drop-Query-Request* packet is sent to the remote peer to negotiate dropping a link. The link will remain active as long as the remote peer considers the link necessary and rejects the *Link-Drop-Query-Request*. A peer can force the dropping of a link without negotiation by sending an LCP *Terminate-Request* packet on the link.

BAP can be configured when a PPP interface is created, using the command:

```
CREATE PPP=ppp-interface OVER=physical-interface BAP={ON|OFF}
    BAPMODE={CALL|CALLBACK}
```

or by modifying an existing PPP interface, using the command:

```
SET PPP=ppp-interface BAP={ON|OFF} BAPMODE={CALL|CALLBACK}
```

By default, BAP is enabled ("ON"). If BAP is disabled, PPP will use the UPRATE, UPTIME, DOWNRATE and DOWNTIME parameters to manage bandwidth on demand (see "*Bandwidth on Demand*" on page 3-9).

Dial-On-Demand

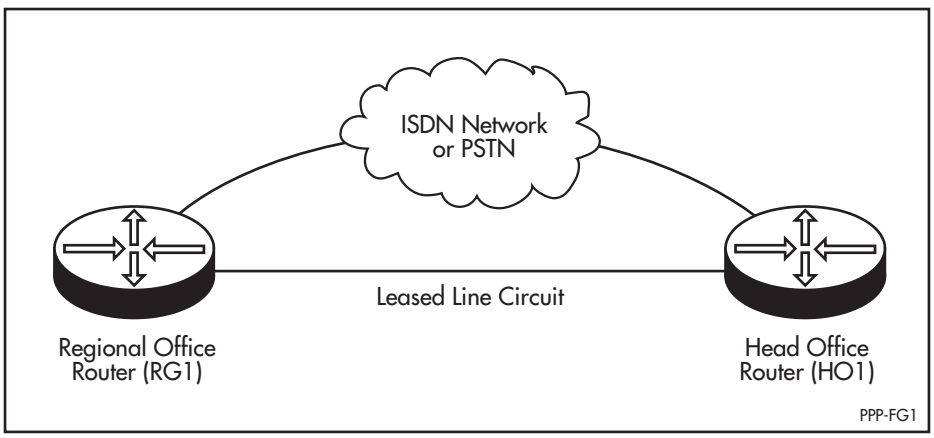
A PPP interface that uses an ISDN or ACC call, or a synchronous port controlling a modem connected to the PSTN, as the physical interface can be configured for dial-on-demand. The call is activated only when there is traffic to transmit over the PPP interface. The call is disconnected when the link has been idle for a period of time specified by the IDLE parameter of the CREATE PPP and SET PPP commands. If the IDLE parameter is set to OFF, the dial-on-demand feature is disabled. The configured and current timer values can be displayed using the command:

```
SHOW PPP IDLETIMER
```

Leased Line Backup

A PPP interface can be configured for leased line backup. The PPP interface must have both a permanent synchronous or TDM link, and either an ISDN link, an ACC link or a synchronous port controlling a modem connected to the PSTN (Figure 3-1 on page 3-8).

Figure 3-1: Example network configuration for leased line backup.



When the permanent synchronous or TDM link fails, LQM detects the failure and resets the link causing configure requests to be transmitted. If the permanent link fails to reach the OPENED state after a number of configure request packets have been transmitted, the backup call is activated and traffic is redirected over the backup link. The number of configure request packets transmitted and the interval between successive retransmissions of configure request packets is controlled by the CONFIGURE and RESTART parameters. PPP con-

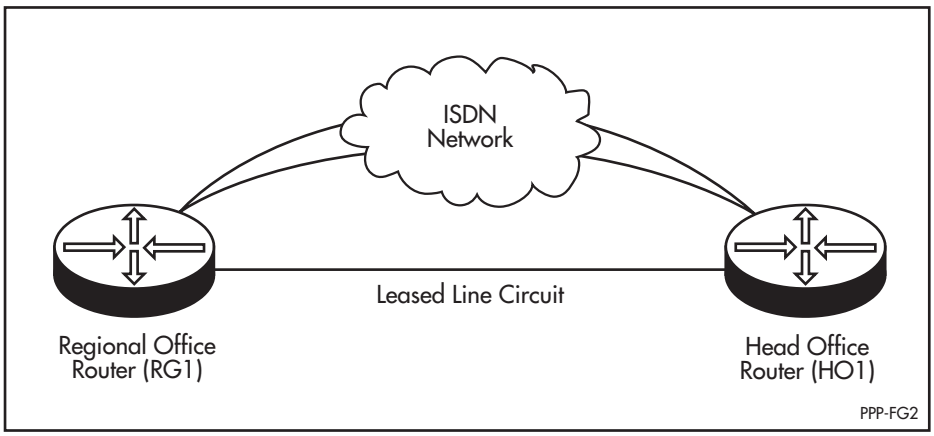
tinually attempts to reopen the permanent link, and when the permanent link is restored, the backup call is deactivated and traffic is redirected over the permanent link again.

When the permanent synchronous or TDM link enters loopback mode, LQR detects the loopback and resets the link. When the link attempts to re-open the negotiation of the Magic Number LCP option will fail and the backup call will be activated. When the link leaves loopback mode the negotiation will finally succeed, the permanent link will reopen, the backup call will be deactivated and traffic will be redirected over the permanent link.

Bandwidth on Demand

A PPP interface over a number of ISDN channels or ACC calls can be configured to provide bandwidth on demand (Figure 3-2 on page 3-9).

Figure 3-2: Example network configuration for bandwidth on demand.



One application of bandwidth on demand is the use of ISDN calls to provide additional bandwidth to a leased line during peak load periods. This application is best suited to a network connection that has a fairly constant load most of the time, but is overloaded during peak periods. A leased line with sufficient capacity to handle the normal loading is supplemented by a connection to an ISDN service. This avoids the high cost of a leased line capable of handling peak loads but which is under-utilised most of the time.

A second application of bandwidth on demand is the use of multiple ISDN connections, instead of a leased line, to provide the bandwidth required at any one time. This application is best suited to a network connection that has a variable and irregular load.

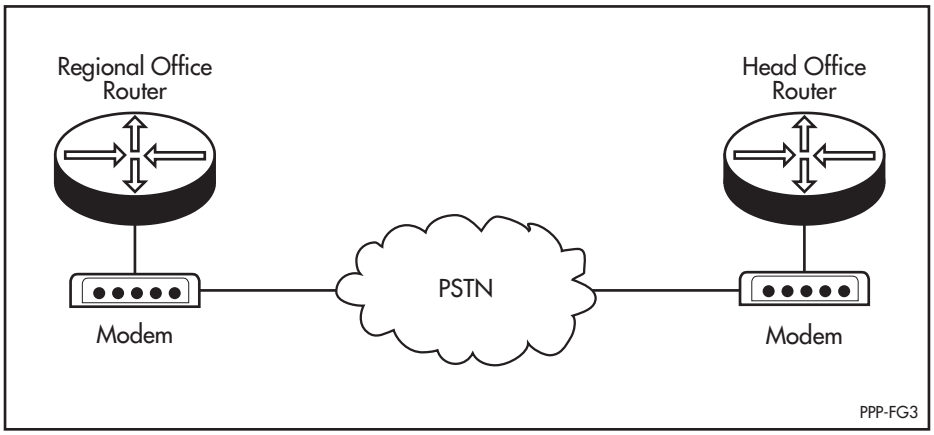
To trigger the addition and removal of channels, the total utilisation of the PPP interface as a percentage of the maximum bandwidth of the PPP interface is measured every second. Each time the utilisation remains above the threshold specified by the UPRATE parameter for a time longer than that specified by the UPTIME parameter, a new ISDN call is made increasing the bandwidth of the PPP interface. When each new link is added the total utilisation of the interface will decrease. However, this decrease will only be momentary if the rate of utilisation is increasing. When the rate of utilisation decreases again, each time the utilisation drops below the threshold specified by the DOWNRATE parameter for a time longer than that specified by DOWNTIME parameter, an ISDN call

will be disconnected and the total bandwidth of the PPP interface will be decreased.

Synchronous Dialling

A PPP interface over a synchronous link can be configured to control a modem connected to the PSTN for router-to-router connections (Figure 3-3 on page 3-10). This functionality, using V.25bis DTR support, enables synchronous dialling to be used as an alternative to ISDN or ACC calls for dial on demand and leased line backup applications.

Figure 3-3: Example network configuration for dial-on-demand using modems.



Synchronous dialing is slower at setting up and taking down calls than ISDN, so the response time for handling events, such as bringing up additional links in a dial on demand application, is longer.

To configure synchronous dialling the MODEM parameter must be set to ON.

The router controls the modem using the modem's DTR input signal. For bidirectional calling each modem must be configured with a number to dial when the DTR signal from the router is raised. Each modem must also be configured to raise the DSR signal to the router when a call has been received and answered.

A modem makes a call when the router to which it is connected asserts DTR. The modem at the remote end of the link will only answer the call if its DTR signal is high. A modem which answers a call will raise its DSR signal to the attached router, which will respond by activating the PPP interface. A call is disconnected when the DTR signal of one of the modems is driven low. These conditions mean that DTR must be idle high so the modem is always ready to answer a call.

To make a call, the router drives DTR low and then high, leaving it ready to drop the call. To drop a call, the router drives DTR low and then high leaving it ready to answer a call. This has the side effect of causing the modem which drops the call to make another call. However, it will encounter an engaged signal as the modem at the remote end of the link will still be off-hook, and it will then hang up.

A potential problem with a bidirectional link is call collisions resulting from both modems attempting to dial each other at the same time. In dial on demand applications, a call collision may occur when traffic to be sent appears at both ends of the link at the same time. In leased line backup applications, a call collision may occur if the failure of the primary link is detected at the routers at each end of the link at the same time. The solution is a simple random backoff scheme. When a call collision occurs, each modem will detect that the remote modem is engaged and will hang up after 15 seconds. The router will detect that the call has failed after 10 seconds and will toggle DTR a random time later. This time will vary between 15 and 45 seconds. If another collision occurs, the routers will back off and try again until one of the modems is able to establish a call. This may take several minutes in the worst case scenario.

Another potential problem occurs when the routers are turned on. DTR will be asserted causing the connected modem to initiate a call. If both routers are powered on at the same time a call collision will occur. In this case the random backoff scheme will not be used, and the modems will hang up after 15 seconds and will not try again. However, if only one router is powered up or reset, the call made will be successful as long as the modem and router at the remote end of the link are switched on. To avoid this extraneous call on power up, it is advisable to turn on each modem only after the router to which it is connected has been powered up.

PPP Callback

The PPP callback feature allows a PPP link to be configured to accept callback requests or to make callback requests. A callback request is made during the LCP negotiation using the LCP callback option which is defined in RFC 1570 as an LCP extension. This option contains a callback operation that specifies how the peer determines the number to use when making the call back and contains a message field whose contents are dependent on the operation being used.

A PPP link is configured to make callback requests with the command:

```
SET PPP=ppp-interface OVER=physical-interface CBMODE=REQUEST
```

A PPP link is configured to accept callback requests with the command:

```
SET PPP=ppp-interface OVER=physical-interface CBMODE=ACCEPT
```

Two types of callback request operations are supported by the router—user authentication and E.164 number. The user authentication callback operation specifies that the number to call back is contained in the User Authentication Database and is obtained during authentication just prior to the call being brought down. To configure user authentication callback, use the command:

```
SET PPP=ppp-interface OVER=physical-interface
   CBOPERATION=USERAUTH
```

The E.164 number operation specifies that the callback number is contained in the message field of the callback option. When the E.164 number operation is configured for requesting a callback, the E.164 number must also be provided. To configure E.164 number callback, use the command:

```
SET PPP=ppp-interface OVER=physical-interface
   CBOPERATION=E164NUMBER CBNUMBER=e164number
```

The CBOPERATION parameter is only valid when the callback mode is set to request callback.

A PPP link that is configured to accept callback requests must also be configured to request authentication. This is necessary to prevent unauthorised peers from requesting a callback.

When a callback request is accepted, and authentication succeeds, the call is brought down and a call is made back to the peer making the request. If authentication fails the link is brought down and no call back is made. In order to cope with any variable delays in bringing down the ISDN call due to any differences in ISDN switches, a delay between bringing down the call and attempting to make the call back can be configured. The units of this delay are tenths of seconds and it is configured using the command:

```
SET PPP=ppp-interface CBDELAY=1..100
```

The CBDELAY parameter is only valid when the callback mode is set to accept callback requests.

Dynamic PPP interfaces can support PPP callback provided the dynamic PPP interface is created using a PPP template in which PPP callback has been configured, for example:

```
CREATE PPP TEMPLATE=9 DESCRIPTION="Dynamic PPP interface with
   callback" CBOPERATION=USERAUTH CBMODE=REQUEST CBDELAY=10
```

The PPP callback feature is currently only supported on PPP links over ISDN calls.

Magic Number

The magic number option is used for loopback detection. A PPP interface that is looped back will not enter the OPENED state if the magic number option is enabled. The magic number option is enabled with the MAGIC parameter of the ADD PPP, CREATE PPP and SET PPP commands.

Authentication Protocols

The PPP Link Control Protocol (LCP) is responsible for establishing, configuring and testing data link connections. Part of the process of configuring a link is the negotiation of various options, including an authentication protocol, which is performed before allowing Network Layer protocols to transmit data over the link. The local device performing the authentication is known as the *authenticator*. The device being authenticated is known as the *peer*.

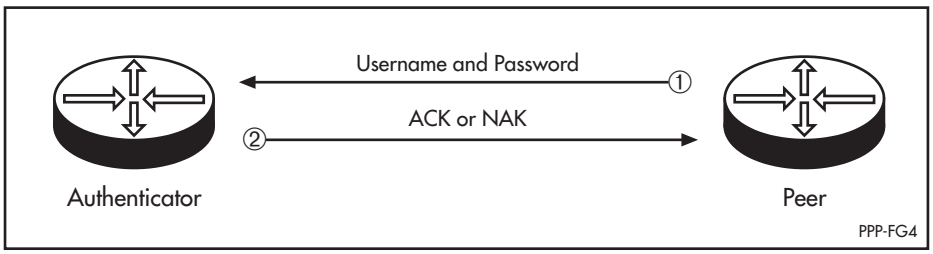
The router supports two authentication protocols: the *Password Authentication Protocol (PAP)* and the *Challenge-Handshake Authentication Protocol (CHAP)*. These protocols are primarily intended for use by PCs and hosts connecting to the router via ISDN calls or modems attached to the asynchronous or synchronous ports of the router, but authentication may also be applied to network connections using dedicated leased lines.

After the PPP link has been established (the Link Establishment phase), an optional Authentication phase will take place before proceeding to the Network-Layer Protocol phase if authentication has been negotiated by the router at either end of the link.

Password Authentication Protocol (PAP)

The Password Authentication Protocol (PAP) is a relatively simple authentication protocol that allows a peer to establish its identity by repeatedly transmitting a user name/password pair to an authenticator until the authenticator acknowledges the peer or terminates the link. The peer requesting authentication controls the process; the authenticator simply responds to requests (Figure 3-4 on page 3-13).

Figure 3-4: The Password Authentication Protocol (PAP) authentication process.



In the case of a PC connecting to the router via an asynchronous modem attached to an asynchronous port, the PC transmits a login name and password which the router compares against entries in the User Authentication Database and any defined TACACS servers.

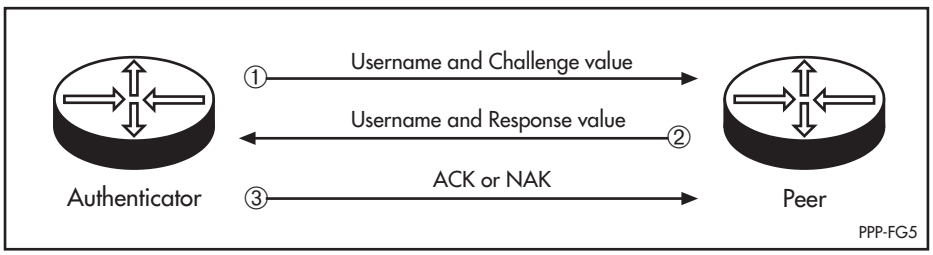
Transmitted passwords are not encrypted, and since the peer always uses the same user name/password pair there is no protection from playback or repeated trial-and-error attacks. PAP provides a similar level of security to a normal remote login.

Challenge-Handshake Authentication Protocol (CHAP)

The Challenge-Handshake Authentication Protocol (CHAP) is a more robust protocol which provides for both authentication during the Link Establishment phase and periodic verification during the Network-Layer Protocol phase.

CHAP is controlled by the authenticator, which sends a *challenge* message containing an identifier and a unique challenge value to the peer. The peer responds with a user name and value calculated by applying a *one-way hash function* (MD5) to a string created by concatenating the identifier, the password for the user name and the challenge value. The authenticator compares the response against its own computation of the function, using the user name to look up the password in the User Authentication Database. If the values match, the authentication is acknowledged, otherwise the link is terminated (Figure 3-5 on page 3-13).

Figure 3-5: The Challenge Handshake Authentication Protocol (CHAP) authentication process.



The challenge is repeated periodically during the Network-Layer Protocol phase to ensure that there has been no change to the link. Each challenge uses a different identifier and challenge value. The identifier value changes in a predictable way (typically the value of a regularly incremented counter), but the challenge value is a unique and random value. The repeated challenges and changing identifier and challenge values provide protection against both playback and trial-and-error attacks. The uniqueness and random nature of the challenge value prevents an attacker from tricking a peer into responding to a challenge then using the response to masquerade as the peer to an authenticator.

CHAP relies on the password being known to both the authenticator and the peer, although the password is not transmitted over the link.

In the case of a PC connecting to the router via an asynchronous modem attached to an asynchronous port, the PC responds to a challenge with a login name and the value of the one-way hash function calculated over the identifier, password and challenge value. The router compares the response to its own calculation of the value, using the clear text encoded login name to retrieve the password from the User Authentication Database. In the case of two routers communicating over a network link, the user name is the user name set for the PPP interface with the USERNAME parameter of the CREATE PPP and SET PPP commands, or if this is not set, the router's system name set with the SET SYSTEM COMMAND (see *Chapter 1, Operation*). The password is the password set for the PPP interface with the PASSWORD parameter of the CREATE PPP and SET PPP commands.

Configuring Authentication

The router can be configured to provide authentication in one of three modes:

- As a peer in a one-way authentication scheme.
- As an authenticator in a one-way authentication scheme.
- As both a peer and an authenticator in a two-way authentication scheme.

Configuring the Router as a Peer

The router can be configured as the peer in a one-way authentication scheme. When the router makes a call to a remote device (e.g. another router configured as an authenticator), it supplies a username and password to the remote device. The remote device will determine whether or not the username and password are valid, and accept or reject the connection. This is the most common PPP authentication configuration. A typical example is a router configured to dial into a remote ISP. The ISP provides clients with a username and password. The ISP's connection server (typically a router) expects the clients router to supply the username and password when it makes a call to the ISP.

The router's username and password (supplied by the ISP) are set using the USERNAME and PASSWORD parameters in the CREATE PPP and SET PPP commands:

```
CREATE PPP=ppp-interface OVER=physical-interface
    USERNAME=username PASSWORD=password
SET PPP=ppp-interface USERNAME=username PASSWORD=password
```

If a username is not set using the PPP commands the peer router's system name is used as the username. The system name is set using the SET SYSTEM command (*see Chapter 1, Operation*). The password can only be set using the PPP commands.

The router will respond to either PAP or CHAP authentication requests by supplying the configured username and password.

Neither PAP or CHAP have been explicitly configured in this example, so the router will not request authentication from remote devices during LCP negotiation. This is appropriate for the example above. Most ISPs configure their connection servers only to request authentication, not to respond to authentication requests. If the client router is configured to request authentication but the ISP's connection server is not configured to respond to authentication requests (as is typical), the ISP's connection server will refuse the connection from the client router and all connection attempts will fail.

Configuring the Router as an Authenticator

The router can be configured as the authenticator in a one-way authentication scheme. When the router receives a call from a remote device (e.g. a user dialling in via a modem or another router configured as a peer), it requests authentication from the remote device. The remote device will supply a username and password which the router will validate before accepting or rejecting the connection. A typical example is an ISP configuring a router to accept dial-in connections from users or other remote devices (routers). The ISP's router will request authentication from the user. The user is expected to reply with the username and password supplied by the ISP when the user signed up for the service.

To configure the router as an authenticator, use the AUTHENTICATION parameter of the CREATE PPP, ADD PPP and SET PPP commands to specify whether or not authentication is required, and if so, which authentication protocol to use:

```
CREATE PPP=ppp-interface OVER=physical-interface
    AUTHENTICATION={NONE|PAP|CHAP|EITHER}
ADD PPP=ppp-interface OVER=physical-interface
    AUTHENTICATION={NONE|PAP|CHAP|EITHER}
SET PPP=ppp-interface OVER=physical-interface
    AUTHENTICATION={NONE|PAP|CHAP|EITHER}
```

The AUTHENTICATION parameter must be set to PAP, CHAP or EITHER and a username and password must be entered in the User Authentication Database for each user PC (or peer) that is allowed to dial in to the router. If PAP is used, the username and password may be stored in a defined TACACS server, instead of the User Authentication Database. If CHAP is used the username and password must be stored in the User Authentication Database. Each peer that wants to connect to the PPP interface on the authenticator must have a username and password configured that matches one of those stored in the User Authentication Database in the authenticator or in a defined TACACS server.

CHAP is not compatible with TACACS because the password is transmitted as plain text between the TACACS server and the router.

The EITHER option uses the PPP option negotiation process to request CHAP authentication. If the peer supports CHAP, CHAP will be used. If the peer does not support CHAP, but does support PAP, PAP will be used. If the peer supports neither authentication protocol then the link is terminated.

Configuring the Router as an Authenticator and a Peer

The router can be configured as both an authenticator and a peer in a two-way authentication scheme. When the router makes a call to a remote device (e.g. another router configured as an authenticator), it supplies a username and password to the remote device. The remote device will determine whether or not the username and password are valid, and accept or reject the connection. When the router receives a call from a remote device (e.g. a user dialling in via a modem or another router configured as a peer), it requests authentication from the remote device. The remote device will supply a username and password which the router will validate before accepting or rejecting the connection. A typical example is two routers configured to communicate via ISDN, a synchronous dial-up connection or an asynchronous dial-up connection. Each router is configured as both a peer and an authenticator, as described in "*Configuring the Router as a Peer*" on page 3-14 and "*Configuring the Router as an Authenticator*" on page 3-15. Either router can make a call to the other router, supplying a username and password as authentication, or accept a call from the other router and request authentication.

The AUTHMODE parameter can be used to control when authentication will be requested. If AUTHMODE is set to INOUT authentication will be requested for both incoming and outgoing calls. Some devices will not accept calls if the calling router also requests authentication from the called router. In this case AUTHMODE can be set to IN so that only incoming calls result in authentication requests.

Debugging PPP Links

Debugging can be enabled or disabled on a PPP interface, using the commands:

```
ENABLE PPP=ppp-interface DEBUG={ALL|AUTH|BAPPKT|BAPSTATE|
   CALLBACK|DEMAND|ENCO|LCP|NCP|PKT|UTILISATION}[,...]
   [PORT=port-number] [TIMEOUT={NONE|1..4000000000}]
   [NUMPKTS={CONT|1..4000000000}]
DISABLE PPP=ppp-interface DEBUG={ALL|AUTH|BAPPKT|BAPSTATE|
   CALLBACK|DEMAND|ENCO|LCP|NCP|PKT|UTILISATION}[,...]
```

Table 3-6 on page 3-51 lists the debugging options and their meanings. Output is sent to the specified asynchronous port or the terminal from which the command was entered.

Templates

Dynamic PPP interfaces are created in response to a request from a lower layer (ISDN, ACC or L2TP) to create a new PPP interface. PPP templates enable the full range of configuration options available on static PPP interfaces to be applied to dynamic PPP interfaces.

A template is a blueprint for the configuration of dynamic PPP interfaces, specifying any of the parameters that may be configured on a static PPP interface. A new template is created using the command:

```
CREATE PPP TEMPLATE=template [COPY=template]
   [AUTHENTICATION={CHAP|EITHER|PAP|NONE}] [BAP={ON|OFF}]
   [BAPMODE={CALL|CALLBACK}] [CBDELAY=1..100]
   [CBMODE={ACCEPT|OFF|REQUEST}] [CBNUMBER=e164number]
   [CBOPERATION={E164NUMBER|USERAUTH}]
   [COMPALGORITHM={PREDICTOR|STACLZS}] [COMPRESSION={ON|OFF|
   LINK}] [DEBUGMAXBYTES=16..256] [DESCRIPTION=description]
   [ECHO={ON|OFF|period}] [ENCRYPTION={ON|OFF}]
   [FRAGMENT={ON|OFF}] [FRAGOVERHEAD=0..100] [IDLE={ON|OFF|
   time}] [IPREQUEST={ON|OFF}] [LOGIN={ALL|RADIUS|TACACS|
   USER}] [LQR={ON|OFF|time}] [MAGIC={ON|OFF}]
   [MAXLINKS=1..64] [NULLFRAGTIMER=time] [PASSWORD=password]
   [PREDCHECK={CRC16|CRCCCITT}] [RESTART=time]
   [STACCHECK={LCB|SEQUENCE}] [STARENTITY=1..255]
   [USERNAME=username]
```

An existing template can be modified or deleted using the commands:

```
SET PPP TEMPLATE=template [AUTHENTICATION={CHAP|EITHER|PAP|
   NONE}] [BAP={ON|OFF}] [BAPMODE={CALL|CALLBACK}]
   [CBDELAY=1..100] [CBMODE={ACCEPT|OFF|REQUEST}]
   [CBNUMBER=e164number] [CBOPERATION={E164NUMBER|USERAUTH}]
   [COMPALGORITHM={PREDICTOR|STACLZS}] [COMPRESSION={ON|OFF|
   LINK}] [DEBUGMAXBYTES=16..256] [DESCRIPTION=description]
   [ECHO={ON|OFF|period}] [ENCRYPTION={ON|OFF}]
   [FRAGMENT={ON|OFF}] [FRAGOVERHEAD=0..100] [IDLE={ON|OFF|
   time}] [IPREQUEST={ON|OFF}] [LOGIN={ALL|RADIUS|TACACS|
   USER}] [LQR={ON|OFF|time}] [MAGIC={ON|OFF}]
   [MAXLINKS=1..64] [NULLFRAGTIMER=time] [PASSWORD=password]
   [PREDCHECK={CRC16|CRCCCITT}] [RESTART=time]
   [STACCHECK={LCB|SEQUENCE}] [STARENTITY=1..255]
   [USERNAME=username]

DESTROY PPP TEMPLATE=template
```

The list of currently defined templates, including the default template, can be displayed using the command:

```
SHOW PPP TEMPLATE
```

The configuration of a specific template can be displayed using the command:

```
SHOW PPP TEMPLATE=template
```

Once a template has been created, it can be associated with an ISDN, ACC or L2TP call using the commands:

```
ADD ACC CALL=name PORT=port-number PPPTEMPLATE=template

SET ACC CALL=name PPPTEMPLATE=template

ADD ISDN CALL=name NUMBER=number PRECEDENCE={IN|OUT}
   PPPTEMPLATE=template

SET ISDN CALL=name PPPTEMPLATE=template

ADD L2TP IP=ipadd-ipadd PPPTEMPLATE=template

DELETE L2TP IP=ipadd-ipadd
```

When the lower layer activates a call that creates a dynamic PPP interface, PPP uses the associated template to create and configure the dynamic PPP interface. If a template has not been specifically associated with a dynamic PPP interface the default template will be used.

The router will not allow configuration templates to be associated with TDM or SYN interfaces.

The full range of PPP debugging options can be enabled or disabled on a PPP template, using the commands:

```
ENABLE PPP TEMPLATE=template DEBUG={ALL|AUTH|BAPPKT|BAPSTATE|
    CALLBACK|DEMAND|ENCO|LCP|NCP|PKT|UTILISATION}[,...]
    [PORT=port-number] [TIMEOUT={NONE|1..4000000000}]
    [NUMPKTS={CONT|1..4000000000}]

DISABLE PPP TEMPLATE=template DEBUG={ALL|AUTH|BAPPKT|
    BAPSTATE|CALLBACK|DEMAND|ENCO|LCP|NCP|PKT|
    UTILISATION}[,...]
```

Table 3-6 on page 3-51 lists the debugging options and their meanings. Any dynamic PPP interface created from a template that has debugging enabled will display the requested debug information. Debugging will cease when the dynamic PPP interface is destroyed.

Support for PPP

The router supports PPP over synchronous links, ISDN calls (see *Chapter 5, Integrated Services Digital Network (ISDN)*), ACC calls (see *Chapter 18, Asynchronous Call Control*), MIOX calls (see *Chapter 6, X.25*), L2TP calls (see *Chapter 27, Layer Two Tunnelling Protocol (L2TP)*) and TDM groups (see *Chapter 22, Time Division Multiplexing (TDM)*), separately and as members of a multilink bundle. PPP can be used on the router to carry IP, IPX, DECnet and AppleTalk routing protocols, bridged protocols, and compressed and/or encrypted data.

A PPP interface is created and associated with a "physical interface" (a synchronous interface, an ISDN call, an ACC call, a MIOX circuit, an L2TP call or a TDM group)

```
CREATE PPP=interface OVER=physical-interface
```

An entire PPP interface can be removed with the command:

```
DESTROY PPP=interface
```

Additional physical interfaces can be added to the PPP interface to form a multilink bundle, using the command:

```
ADD PPP=interface OVER=physical-interface
```

If an ISDN call is being added as the physical interface, multiple physical interfaces can be added using the NUMBER parameter. For example, the following command adds two identical ISDN calls (named "HeadOffice") as physical interfaces to PPP interface 0:

```
ADD PPP=0 OVER=ISDN-HeadOffice NUM=2
```

Members of a multilink bundle can be selectively deleted with the command:

```
DELETE PPP=interface OVER=physical-interface
```

An entire PPP interface can be temporarily disabled or enabled, or reset, with the commands:

```
DISABLE PPP=interface
ENABLE PPP=interface
RESET PPP=interface
```

One of the features of PPP is the negotiation of options for each protocol using the link. All options have a default value to which the option will be set if either end of the PPP link does not wish the option to be different from the default. The LCP will attempt to negotiate the Maximum Receive Unit (MRU), Authentication Protocol, Link Quality Reporting (LQR), Magic Number, Asynchronous Control Character Map (ACCM) and Maximum Received Reconstructed Unit (MRRU) options. All other possible options are set to the default values specified in the relevant RFC.

The IP NCP will attempt to negotiate Van Jacobson's TCP/IP header compression if this has been turned on with the command:

```
ADD IP INTERFACE... VJC=ON
```

For more information on turning on Van Jacobson's TCP/IP header compression, see *Chapter 8, Internet Protocol (IP)*.

Van Jacobson's TCP/IP header compression should not be enabled on a multilink PPP interface.

The IP NCP will also negotiate the IP Address option. This option is used to inform each end of the link what the IP address of the other end of the link is by passing the address to the peer inside the option.

If the PPP interface has an IP address of 0.0.0.0 defined it may request an IP address from the peer by passing an IP address of 0.0.0.0 to the peer. If the peer has an IP address to allocate it will pass this IP address to the requesting router in a IPCP Configure Nak packet. To configure the router to request an IP address using the IP address option, use the commands:

```
SET PPP=ppp-interface IPREQUEST=ON
SET IP INT=ppp-interface IPADDRESS=0.0.0.0
ENABLE IP REMOTEASSIGN
RESET IP
```

The IP NCP also provides a number of options for requesting name server addresses from the peer. These name server addresses consist of primary and secondary DNS and WINS (*Windows Internet Name Service*) server addresses. The router will only request the primary DNS address from a peer, but will supply the peer with primary and secondary DNS and WINS server addresses if a request is made. The values to be supplied to the peer are set using the command:

```
SET PPP [DNSPRIMARY=ipadd] [DNSSECONDARY=ipadd]
    [WINSPRIMARY=ipadd] [WINSSECONDARY=ipadd]
```

The router supports both the CHAP and PAP authentication protocols through the AUTHENTICATION parameter of the ADD PPP, CREATE PPP and SET PPP commands:

```
CREATE PPP=ppp-interface OVER=physical-interface
    AUTHENTICATION={NONE|PAP|CHAP|EITHER}
ADD PPP=ppp-interface OVER=physical-interface
    AUTHENTICATION={NONE|PAP|CHAP|EITHER}
SET PPP=ppp-interface OVER=physical-interface
    AUTHENTICATION={NONE|PAP|CHAP|EITHER}
```

The router supports the link quality management options for PPP through the LQR parameter of the ADD PPP, CREATE PPP and SET PPP commands:

```
ADD PPP=0 OVER=SYN0 LQR=ON
```

A PPP interface can be configured for dial-on-demand operation by specifying the IDLE parameter in the CREATE PPP or SET PPP commands:

```
CREATE PPP=0 OVER=ISDN-HeadOffice NUM=2 IDLE=ON
```

A PPP interface can be configured for leased line backup by specifying the TYPE parameter in the ADD PPP, CREATE PPP and DELETE PPP commands:

```
CREATE PPP=0 OVER=SYN0 CONF=5
ADD PPP=0 OVER=ISDN-HeadOffice NUM=2 TYPE=SECONDARY
```

A PPP interface can be configured for bandwidth on demand by specifying the TYPE parameter in the ADD PPP, CREATE PPP and DELETE PPP commands, and the UPRATE, UPTIME, DOWNRATE and DOWNTIME parameters in the CREATE PPP and SET PPP commands:

```
CREATE PPP=0 OVER=ISDN-HeadOffice NUM=2 IDLE=ON TYPE=DEMAND
   UPRATE=60 UPTIME=30 DOWNRATE=20 DOWNTIME=30
```

A PPP interface can be configured to control a modem via a synchronous port by specifying the MODEM parameter in the ADD PPP, CREATE PPP and DELETE PPP commands:

```
CREATE PPP=0 OVER=SYN0 IDLE=ON MODEM=ON
```

A PPP interface can be configured to provide AODI (*Always On/Dynamic ISDN*) by specifying a MIOX circuit as the primary link and an ISDN call as the demand link in the ADD PPP and CREATE PPP commands:

```
CREATE PPP=0 OVER=MIOX3-AODI IDLE=40000000

ADD PPP=0 OVER=ISDN-AODI TYPE=DEMAND NUM=2
```

See "*Always On/Dynamic ISDN (AODI)*" on page 5-40 of *Chapter 5, Integrated Services Digital Network (ISDN)* for more information about configuring AODI.

The router uses a number of counters and timers to control the LCP and NCPs. The timers control the retransmission of *Configure-Request* and *Terminate-Request* control protocol packets. If the correct acknowledgement is not seen in the timeout period, another packet is transmitted. Counters control the number of times the packets can be sent. The *Configure* counter records retransmissions of *Configure-Requests*. If this counter exceeds the value set for it, the LCP will reset the interface and start again. The *Terminate* counter records retransmissions of *Terminate-Requests*. If this counter exceeds the value set for it, the link is assumed to be DOWN. The *Failure* counter is used to control the number of attempts to reach an agreeable set of values for options being negotiated by an NCP. This counter is not used in the router.

The values for the timers and counters can be set with the ADD, CREATE or SET commands.

Interface parameters can be modified after the interface has been created, with the command:

```
SET PPP=interface parameter=value...
```

The command:

```
SHOW PPP[=interface] [CONFIGURATION|COUNT|IDLETIMER|
   MULTILINK]
```

displays information about a PPP interface. If CONFIGURATION is specified, the settings of configuration parameters such as LQR and restart timers are displayed. If COUNT is specified, counters from the interface MIB and counters for the users of the interface are displayed. If IDLETIMER is specified, the con-

figured and current values of the idle timer are displayed. If MULTILINK is specified, information about the multilink bundle associated with the interface is displayed. The display includes the number of links in the bundle, the number of packets fragmented, the number of packets or fragments in the multilink receive queue, and information about the sequence numbers on the multilink bundle. If no optional parameters are specified, a summary of the configured PPP interfaces, the physical interfaces used and the Network Control Protocols (NCPs) in use is displayed.

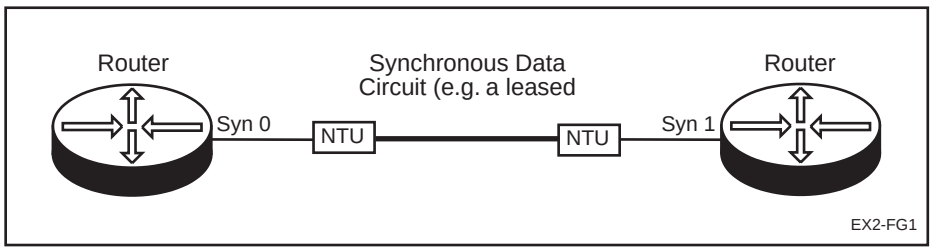
Configuration Examples

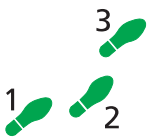
The following examples illustrate some of the options available for configuring PPP interfaces to provide a range of network services.

Configuring a PPP link

In this example, a Point-to-Point Protocol (PPP) link will be set up between two routers (Figure 3-6 on page 3-21). The function of PPP is to maintain a channel between the routers, over which data can be exchanged. To exchange data, the relevant routing module(s) must be assigned to use a PPP link.

Figure 3-6: Example network for configuring a PPP link.





To configure a PPP link:

1. Connect the routers to the Data Circuit

   Ensure that the NTUs or modems are correctly installed on the data circuit—try a remote loop back.

   Using the correct cables connect the synchronous interface on each router (synchronous interface 0 on Router A, synchronous interface 1 on Router B) to the local NTU or modem. Contact your dealer if you are unsure which cables to use.

2. Create the PPP interface.

   On Router A, create a PPP interface numbered 0 over synchronous port 0:

   ```
   CREATE PPP=0 OVER=SYN0
   ```

   On Router B, create a PPP interface numbered 1 over synchronous port 1:

   ```
   CREATE PPP=1 OVER=SYN1
   ```

   The PPP interface is enabled by default when it is created.

To configure additional PPP links, repeat the above commands for each additional PPP link. Each PPP interface on a router has a unique number and can run over different synchronous interfaces. For example, PPP7 could run over SYN3. However, keeping the

interface numbers the same as the physical port numbers wherever possible makes management easier.

Additional physical interfaces can be added to the PPP interface to form a multilink bundle, using the ADD PPP command. For example, a PPP interface may also be created to use an ISDN call as a physical interface. The ISDN call must have been defined previously using the command:

```
ADD ISDN CALL=demand NUM=23432 PREC=IN
```

To add the ISDN call "demand" as a physical interface to the PPP interface created above, on Router A use the command:

```
ADD PPP=0 OVER=ISDN-demand
```

On Router B, use the command:

```
ADD PPP=1 OVER=ISDN-demand
```

The PPP interface may be configured for dial on demand operation by adding the IDLE=ON option to the CREATE commands, or the option may be set at a later date with the SET command:

```
SET PPP=0 IDLE=ON
```

3. Enable routing modules to use the interface.

Once a PPP interface has been defined and configured, routing modules can be configured to use the interface. The procedures for achieving this are described in the chapter for the particular routing module.

In general, commands that contain the parameter INTERFACE= can refer to a PPP interface by name. The form of the name is "ppp*n*", where *n* is the interface number for the PPP module. Examples of commands that can refer to a PPP interface include:

```
ADD IP INTERFACE=PPPn...
ADD IPX CIRCUIT INTERFACE=PPPn...
ADD DECNET INTERFACE=PPPn...
ADD APPLE PORT=PPPn...
```

As an example, the IP routing module is to use the PPP interface just configured. The RIP routing protocol is to be used, so the PPP link has to be assigned its own an IP subnet. Use of OSPF as the routing protocol would mean that the PPP link could be set up as a unnumbered link. The subnet assigned to the PPP link is 172.16.254.0, with 255.255.255.0 as the subnet mask. The local (Router A) end of the link will have address 172.16.254.1, and the remote (Router B) end will have address 172.16.254.2. RIP is to be enabled to the remote end of the link. Router A already has an IP interface for the Ethernet interface, with an IP address of 172.16.9.59. The commands for Router A are:

```
ENABLE IP
ADD IP INT=PPP0 IP=172.16.254.1 MASK=255.255.255.0
ADD IP RIP INT=PPP0
```

4. Test that the link is active.

The PPP interface can be checked with the command:

```
SH PPP
```

which produces a display like Figure 3-7 on page 3-23. For each control protocol (listed in the *CP* field), the corresponding *State* field should be set to 'OPENED'.

Figure 3-7: Example output from the SHOW PPP command for a PPP link.

```
Name            Enabled  ifIndex  Over                  CP          State
------------------------------------------------------------------------
ppp0              YES      04                           IPCP        OPENED
                                    syn0                 LCP         OPENED
                                    isdn-demand          LCP         OPENED
------------------------------------------------------------------------
```

If the LCP has a state that is not 'OPENED' check the configuration of the physical interfaces used by the PPP interface. Check that the cables connecting the synchronous ports to the local NTUs or modems are the correct type. Contact your dealer for assistance.

Check the NTUs or modems are correctly installed. Perform a remote loop back from each end alternately. Contact the Telecom supplier or your dealer if this fails.

Some modems or NTUs may require signals which are not provided by the router directly. These can usually be 'strapped' internal to the NTU or modem by the Telecom supplier or external wire jumpers can be added to the cable. Check with the Telecom supplier or your dealer.

Check that the synchronous ports have been configured correctly for the network to which they are connected. Check the synchronous interface counters for high link error rates using the command:

```
SHOW SYN=0 COUNTERS
```

The counters that usually increase with high link error are the *Aborts*, *CRCErrors* and *UnderlengthFrames* counters. See *Chapter 2, Interfaces* for a detailed description of these counters. The error counters should be low in relation to the good frame counters. The *seconds* counter gives the length of time that the counters have been active and can be used to assess the quality of the link.

It is normal for most serial wide area links to have a low error rate. Check with the Telecom supplier for an estimate of what they regard as acceptable.

To try to resolve this situation, consider the following possibilities:

1. This circuit may be faulty. Ask the Telecom supplier to test it.
2. This could be caused by poor quality or overlong cables, especially at higher link speeds. This will probably not be a factor below 1–2Mbps link speeds. Contact your dealer for assistance.

For a PPP interface that is using an ISDN call as the physical interface, check that the calls have been properly defined and are active on the routers at each end of the link.

If the routing protocol is not in the state 'OPENED' check the configuration of the routing module. As a first step, the IP configuration can be checked with the command:

```
SHOW IP INTERFACE
```

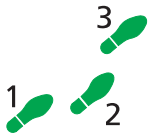
which produces a display like Figure 3-8 on page 3-24.

Figure 3-8: Example output from the SHOW IP INTERFACE command for a PPP link configured for use by the IP routing module.

```
Interface     Type      IP Address       Bcast  PArp  Filt  RIP Metric   SAMode
Pri. Filt     Pol.Filt  Network Mask     MTU    VJC   GRE   OSPF Metric  SACache
-------------------------------------------------------------------------------
LOCAL         -         Not Set          -      -     ---   -            -
---           ---       -                -      -     ---   -            -
eth0          Static    202.36.163.36    1      On    ---   01           Pass
---           ---       255.255.255.0    1500   -     ---   0000000001   None
ppp0          Static    192.168.1.1      1      -     ---   01           Pass
---           ---       255.255.255.0    1500   Off   ---   0000000001   None
ppp1          Static    192.168.2.1      1      -     ---   01           Pass
---           ---       255.255.255.0    1500   Off   ---   0000000001   None
-------------------------------------------------------------------------------
```

Multilink Aggregation

Traffic can be sent over multiple physical interfaces using PPP multilink. A PPP interface is created and configured to use more than one physical interface (e.g. ISDN B channels or synchronous ports). Any combination of physical interface types may be used (e.g. two ISDN B channels, or one ISDN B channel and a synchronous port, or three synchronous ports). This example expands on "*A Basic ISDN Setup*" on page 5-44 of *Chapter 5, Integrated Services Digital Network (ISDN)*, by aggregating traffic on two ISDN B channels between router HO1 and RG1.



To configure channel aggregation on a PPP interface:

1. Set up the ISDN call.

   Create an ISDN call between routers HO1 and RG1 as in "*A Basic ISDN Setup*" on page 5-44 of *Chapter 5, Integrated Services Digital Network (ISDN)*.

2. Create a PPP interface to use the ISDN call.

   Create a PPP interface to use the ISDN call Region1 twice (i.e. activate two calls using the same call definition). On the Head Office router, create PPP0 to use ISDN call Region1:

   ```
   CREATE PPP=0 OVER=ISDN-Region1 NUM=2 IDLE=ON
   ```

   On the Region 1 router, create PPP0 to use the ISDN call HeadOffice twice:

   ```
   CREATE PPP=0 OVER=ISDN-Region1 NUM=2 IDLE=ON
   ```

3. Configure routing modules to use the PPP interface.

   Configure one or more routing modules to use the PPP interface. See "*A Basic ISDN Setup*" on page 5-44 of *Chapter 5, Integrated Services Digital Network (ISDN)*.

4. Test the configuration.

   The PPP configuration can be checked using the command:

   ```
   SHOW PPP
   ```

   The expected output is shown in Figure 3-9 on page 3-25. All control protocols should have their State set to 'OPENED'. If either PPP LCP is not in the 'OPENED' state, check that the ISDN calls are active on both routers. If any of the routing control protocols (in this case IPCP) is not in the 'OPENED' state check the configuration of the routing module on both routers.

Figure 3-9: Example output from the SHOW PPP command for a PPP interface aggregated over two ISDN B channels.

```
Name            Enabled  ifIndex  Over                  CP          State
-------------------------------------------------------------------------
ppp0              YES      04                           IPCP        OPENED
                                    isdn-Region1         LCP         OPENED
                                    isdn-Region1         LCP         OPENED
-------------------------------------------------------------------------
```

The ISDN calls can be checked using the command:

```
SHOW ISDN CALL
```

The expected output is shown in Figure 3-10 on page 3-25. There should be two active calls with the State field set to 'ON'. If not, the calls can be attempted again either by deactivating and then reactivating them, or by resetting the interface. For the HO1 router the commands are:

```
DEACTIVATE ISDN CALL=Region1
ACTIVATE ISDN CALL=Region1
ACTIVATE ISDN CALL=Region1
```

or:

```
RESET PPP=0
```

*The DEACTIVATE command deactivates **all** calls with the specified name. In this example, PPP has been configured to make two Region1 calls. The DEACTIVATE command will deactivate (hang up) both calls. The ACTIVATE command makes a single call based on the specified call definition. To reactivate both calls for this example, the ACTIVATE command must be used twice.*

Figure 3-10: Example output from the SHOW ISDN CALL command for a PPP interface aggregated over two ISDN B channels.

```
ISDN call details
Name             Number            Remote call      State    Precedence
-------------------------------------------------------------------------
Region1          043332345         -                IN & OUT    OUT
-------------------------------------------------------------------------

ISDN active calls
Index   Name              User     State  Prec
-------------------------------------------------------------
   0    Region1           03-00    ON     Yes
   1    Region1           03-36    ON     Yes
-------------------------------------------------------------
```

Dial on Demand Links

A PPP interface can be configured so that it only brings the link up when there is traffic to send. This feature is only useful on switched interfaces (e.g. ISDN) because for other types the physical layer is available all the time. This feature is sometimes called dial on demand. The link is disconnected when there has been no traffic for a specified period of time. This feature is disabled by default. The follow examples assume PPP interface 0 has been configured as in "*A Basic ISDN Setup*" on page 5-44 of *Chapter 5, Integrated Services Digital Network (ISDN)*.

To enable dial-on-demand and use the default disconnect timer (60 seconds), use the command:

```
SET PPP=0 IDLE=ON
```

To enable dial-on-demand with the disconnect timer set to 20 seconds, use the command:

```
SET PPP=0 IDLE=20
```

To disable dial-on-demand, use the command:

```
SET PPP=0 IDLE=OFF
```

To check the configuration, use the command:

```
SHOW PPP=0 CONF
```

Link Quality Monitoring

Link quality monitoring is used to measure the quality of a link. The protocol used is an option negotiated when the link is brought up. There is only one protocol for this, Link Quality Report. Packet and octets loss count, and link failure can be determined using LQR. The negotiation process determines how often a router should receive an LQR packet on a PPP interface. If a router does not receive two consecutive LQR packets within the specified time frame it will reset the link. When using an ISDN call with the PPP interface this will disconnect the call if it is connected and try to reconnect it.

The LQR counters can be displayed with the command:

```
SHOW PPP=0 COUNT
```

and the network manager can decide whether the level of packet and octet loss is good or bad. In a multilink configuration, LQR can be configured differently on each physical interface in the multilink bundle. The following examples assume PPP interface 0 has been configured as in "*A Basic ISDN Setup*" on page 5-44 of *Chapter 5, Integrated Services Digital Network (ISDN).*

To enable LQR with the default timer (60 seconds), use the command:

```
SET PPP=0 OVER=ISDN-HeadOffice LQR=ON
```

To enable LQR with the timer set to 20 seconds, use the command:

```
SET PPP=0 OVER=ISDN-HeadOffice LQR=20
```

To disable LQR, use the command:

```
SET PPP=0 OVER=ISDN-HeadOffice LQR=OFF
```

To check the configuration, use the command:

```
SHOW PPP=0 CONF
```

Compression and Encryption

PPP interfaces can be configured to use the ENCO coprocessor engine or MAC card to provide compression and/or encryption over wide area links. See *Chapter 15, Compression and Encryption* for more information. Compression must be configured on per-interface basis, on the routers at both ends of the PPP link. For PPP multilink interfaces, the data may be compressed before the packets are forwarded to the multilinking process (COMP=ON), in which case all packets on all member links of the multilink carry compressed data, or the data may be compressed after the packets are forwarded to the multilinking process (COMP=LINK), in which case only packets on the specified member link of the multilink carry compressed data. The following example commands illustrate some of the options for enabling compression.

To create a PPP interface aggregating synchronous port 0 and synchronous port 1 with compression enabled only on synchronous port 1, use the commands:

```
CREATE PPP=0 OVER=SYN0
ADD PPP=0 OVER=SYN1 COMP=LINK
```

To change the compression from synchronous port 1 to synchronous port 0, use the commands:

```
SET PPP=0 OVER=SYN1 COMP=OFF
SET PPP=0 OVER=SYN0 COMP=LINK
RESET PPP=0
```

To enable compression before aggregation, use the commands:

```
SET PPP=0 COMP=ON
RESET PPP=0
```

To disable compression, use the commands:

```
SET PPP=0 COMP=OFF
RESET PPP=0
```

To check any of these configurations, use the command:

```
SHOW PPP CONFIG
```

Encryption must be configured on per-interface basis, on the routers at both ends of the PPP link. A star entity must be associated with the PPP interface, and specifies the encryption algorithm to use. See "*STAR Key Management*" on page 15-14 of *Chapter 15, Compression and Encryption* for more information about creating star entities. Encryption can be enabled either when a PPP interface is created or by modifying the configuration of an existing PPP interface, using the commands:

```
CREATE PPP=ppp-interface OVER=physical-interface
   ENCRYPTION=ON STARENTITY=1..255

SET PPP=ppp-interface OVER=physical-interface ENCRYPTION=ON
   STARENTITY=1..255
```

The Encryption Control Protocol (ECP) defined in RFC 1968 is used to negotiate encryption options with the remote peer. During ECP negotiation, ECP option 0 is used to offer the peer the encryption algorithm configured in the associated star entity. If the star entity associated with the peer is not configured with the same encryption algorithm, the option will be rejected, the negotiation will fail, and the link will be closed.

Leased Line Backup

A PPP interface can be configured to use an ISDN call to back up a synchronous (leased) line. When a link is added to a PPP interface it can be assigned a channel type of PRIMARY or SECONDARY. The default channel type is PRIMARY. To perform leased line backup the PPP link using the synchronous line must be assigned a channel type of PRIMARY and the PPP link using the ISDN must be assigned a channel type of SECONDARY. When a primary link failure is detected (by LQR) it is reset and an attempt is made to reopen the link. If the LCP of the primary link fails to reach the OPENED state after sending a number of configure requests, the secondary link is activated. The primary link will continually attempt to reopen and when it succeeds it closes the secondary link. The CONFIGURE parameter specifies the number of configure requests required before the secondary link is activated, and defaults to CONTINUOUS. The RESTART parameter controls how often configure requests are transmitted and defaults to 3 seconds. To enable lease line backup, the CONFIGURE parameter needs to be set to a value other than CONTINUOUS (e.g. 5).

This example illustrates how to configure leased line backup between two routers (Figure 3-11 on page 3-28, Table 3-3 on page 3-28).

Figure 3-11: Example configuration for leased line backup.

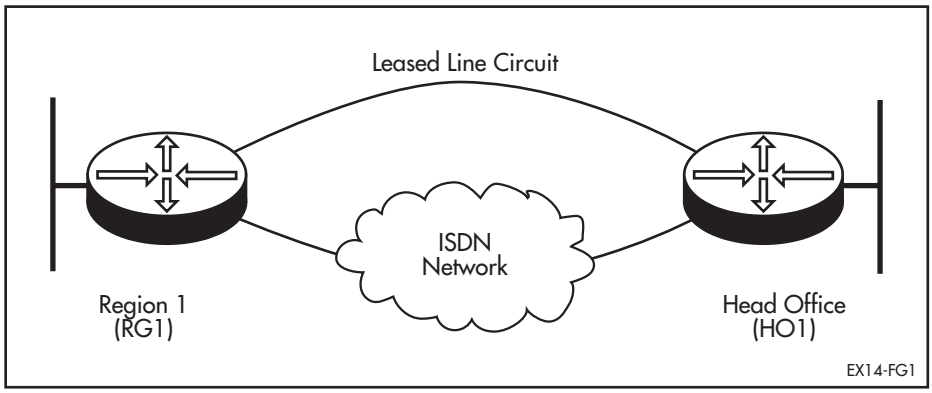


Table 3-3: Example configuration parameters for leased line backup.

Site	Region 1	Head Office
Router Name	RG1	HO1
ISDN Number	1234567	9876543
IP Address for PPP0	192.168.35.114	192.168.35.113
IP Address for Eth0	192.168.35.110	192.168.35.45
Subnet Mask	255.255.255.240	255.255.255.240

To configure leased line backup:

1. Create the ISDN calls.

   An ISDN call must be defined on each router so that either router may initiate a call to transfer data. For a more detailed example of creating ISDN calls see *"A Basic ISDN Setup"* on page 5-44 of *Chapter 5, Integrated Services Digital Network (ISDN)*.

   Set the ISDN call profile appropriate for the ISDN service provider. The default profile is the ETSI specification for European Union (EU) countries

(ETB for Basic Rate interfaces or ETP for Primary Rate interfaces). To use the Australian Telecom profile, for example, on Basic Rate interface BRI 0 for router HO1 and RG1, use the following command on each router:

```
SET Q931=BRI0 PROFILE=AUS
```

On the Head Office router, create a call to the Region 1 router:

```
ADD ISDN CALL=Region1 PREC=IN OUTSUB=LOCAL SEARCHSUB=LOCAL
   NUMBER=1234567
```

On the Region 1 router create a call to the Head Office router:

```
ADD ISDN CALL=Region1 PREC=OUT OUTSUB=LOCAL
   SEARCHSUB=LOCAL NUMBER=9876543
```

2. Create a PPP interface over the synchronous interface.

   Create the PPP interface, setting the CONFIGURE parameter to 5 and the LQR timer to 10 seconds. This speeds up link failure detection as the default is 60 seconds. The default link type is PRIMARY. On the Head Office router create a PPP interface:

   ```
   CREATE PPP=0 OVER=SYN0 CONF=5 LQR=10
   ```

   On the Region 1 router create a PPP interface:

   ```
   CREATE PPP=0 OVER=SYN0 CONF=5 LQR=10
   ```

3. Add the ISDN calls to the PPP interface.

   Add the ISDN calls, specifying a link type of SECONDARY. On the Head Office router add an ISDN call:

   ```
   ADD PPP=0 OVER=ISDN-Region1 TYPE=SECONDARY
   ```

   On the Region 1 router add an ISDN call:

   ```
   ADD PPP=0 OVER=ISDN-Region1 TYPE=SECONDARY
   ```

4. Configure IP.

   Configure a routing module to use the PPP interfaces. It could be IPX, DECnet, AppleTalk or bridging but for this example IP is used. Configure IP at the Head Office router:

   ```
   ENABLE IP
   ADD IP INT=ppp0 IP=192.168.35.113 MASK=255.255.255.240
   ```

   Configure IP at the Region 1 router:

   ```
   ENABLE IP
   ADD IP INT=ppp0 IP=192.168.35.114 MASK=255.255.255.240
   ```

   For a more detailed example of configuring IP see "*Configuration Examples*" on page 8-35 of *Chapter 8, Internet Protocol (IP)*.

Bandwidth on Demand

A PPP interface can be configured to use up to two B channels on a Basic Rate ISDN interface, or up to 30 B channels on a Primary Rate ISDN interface, to provide bandwidth on demand. PPP activates channels when the bandwidth used exceeds an upper threshold and deactivates channels when the bandwidth used drops below a lower threshold. To configure bandwidth on demand the ISDN channels are assigned a TYPE of DEMAND when added to the PPP interface. Assigning one channel a type of PRIMARY and other channels a TYPE of DEMAND will ensure that there is always one channel available. If all channels are assigned a TYPE of DEMAND then there will be no

channels active when there is no traffic; some traffic will cause one channel to be activated and continuous traffic will cause other channels to be activated. If there is one channel remaining opened then the IDLE timer is used to determine when this should be closed. In this case the IDLE timer should not be set to OFF.

This example illustrates how to configure bandwidth on demand between two routers (Figure 3-12 on page 3-30, Table 3-4 on page 3-30).

Figure 3-12: Example configuration for bandwidth on demand.

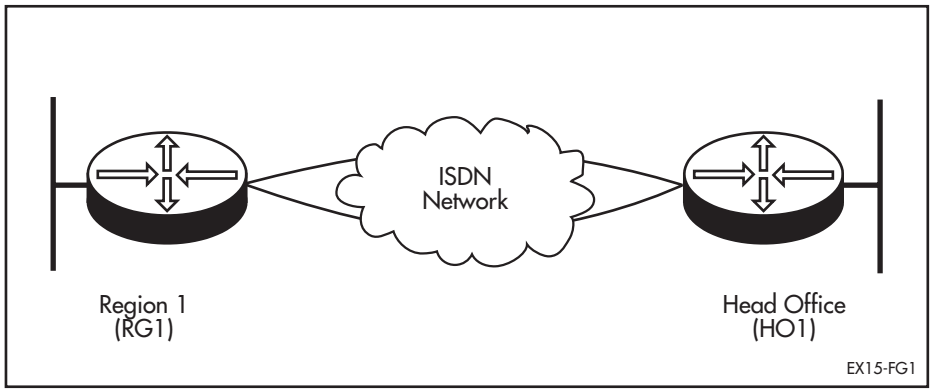
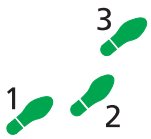


Table 3-4: Example configuration parameters for bandwidth on demand.

Site	Region 1	Head Office
Router Name	RG1	HO1
ISDN Number	1234567	9876543
IP Address for PPP0	192.168.35.114	192.168.35.113
IP Address for Eth0	192.168.35.110	192.168.35.45
Subnet Mask	255.255.255.240	255.255.255.240



To configure PPP for bandwidth on demand:

1. **Create the ISDN calls.**

   An ISDN call must be defined on each router so that either router may initiate a call to transfer data. For a more detailed example of creating ISDN calls see "*A Basic ISDN Setup*" on page 5-44 of *Chapter 5, Integrated Services Digital Network (ISDN)*.

   Set the ISDN call profile appropriate for the ISDN service provider. The default profile is the ETSI specification for European Union (EU) countries (ETB for Basic Rate interfaces or ETP for Primary Rate interfaces). To use the Australian Telecom profile, for example, on Basic Rate interface BRI 0 for router HO1 and RG1, use the following command on each router:

   ```
   SET Q931=BRI0 PROFILE=AUS
   ```

   On the Head Office router, create calls to the Region 1 router:

   ```
   ADD ISDN CALL=Region1 PREC=IN OUTSUB=LOCAL SEARCHSUB=LOCAL
       NUMBER=1234567
   ADD ISDN CALL=Demand PREC=IN OUTSUB=LOCAL SEARCHSUB=LOCAL
       NUMBER=1234567
   ```

   On the Region 1 router create calls to the Head Office router:

```
ADD ISDN CALL=Region1 PREC=OUT OUTSUB=LOCAL
    SEARCHSUB=LOCAL NUMBER=9876543
ADD ISDN CALL=Demand PREC=OUT OUTSUB=LOCAL SEARCHSUB=LOCAL
    NUMBER=9876543
```

2. Create a PPP interface to use the ISDN calls.

   Create the PPP interface with one primary channel and one demand channel. The primary channel is created with the IDLE parameter ON (defaults to 60 seconds). The demand channel is added with the TYPE parameter set to DEMAND. On the Head Office router create a PPP interface:

   ```
   CREATE PPP=0 OVER=ISDN-Region1 IDLE=ON
   ADD PPP=0 OVER=ISDN-Demand TYPE=DEMAND
   ```

   On the Region 1 router create a PPP interface:

   ```
   CREATE PPP=0 OVER=ISDN-Region1 IDLE=ON
   ADD PPP=0 OVER=ISDN-Demand TYPE=DEMAND
   ```

3. Configure IP.

   Configure a routing module to use the PPP interfaces. It could be IPX, DECnet or bridging but for this example IP is used. Static routes must be defined with on-demand links because a routing protocol would keep a link up continuously. Configure IP at the Head Office router:

   ```
   ENABLE IP
   ADD IP INT=ppp0 IP=192.168.35.113 MASK=255.255.255.240
   ADD IP ROUTE=192.168.35.96 INT=ppp0 NEXT=192.168.35.114
      MET=2
   ```

   Configure IP at the Region 1 router:

   ```
   ENABLE IP
   ADD IP INT=ppp0 IP=192.168.35.114 MASK=255.255.255.240
   ADD IP ROUTE=192.168.35.0 INT=ppp0 NEXT=192.168.35.113
      MET=2 MASK=255.255.255.0
   ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXT=192.168.35.113 MET=3
   ```

   For a more detailed example of configuring IP see "*Configuration Examples*" on page 8-35 of *Chapter 8, Internet Protocol (IP)*.

Bandwidth on Demand with Leased Line Circuits and ISDN

A PPP interface can be configured to use a number of ISDN channels to provide bandwidth on demand. PPP activates channels when the bandwidth used exceeds an upper threshold and deactivates channels when the bandwidth used drops below a lower threshold. To configure bandwidth on demand the ISDN channels are assigned a TYPE of DEMAND when added to the PPP interface. Assigning one channel a type of PRIMARY and other channels a TYPE of DEMAND will ensure that there is always one channel available. If all channels are assigned a TYPE of DEMAND then there will be no channels active when there is no traffic; some traffic will cause one channel to be activated and continuous traffic will cause other channels to be activated. If there is one channel remaining opened then the IDLE timer is used to determine when this should be closed. In this case the IDLE timer should not be set to OFF.

This example illustrates how to configure bandwidth on demand between two routers (Figure 3-13 on page 3-32, Table 3-5 on page 3-32).

Figure 3-13: Example configuration for bandwidth on demand with leased line circuits and ISDN.

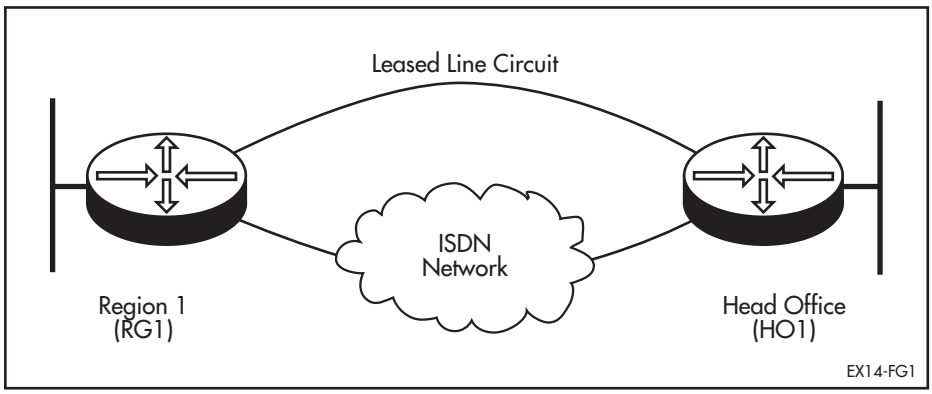
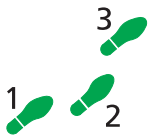


Table 3-5: Example configuration parameters for bandwidth on demand with leased line circuits and ISDN.

Site	Region 1	Head Office
Router Name	RG1	HO1
ISDN Number	1234567	9876543
IP Address for PPP0	192.168.35.114	192.168.35.113
IP Address for Eth0	192.168.35.110	192.168.35.45
Subnet Mask	255.255.255.240	255.255.255.240



To configure bandwidth on demand with leased line circuits and ISDN:

1. **Create the ISDN calls.**

   An ISDN call must be defined on each router so that either router may initiate a call to transfer data. For a more detailed example of creating ISDN calls see "*A Basic ISDN Setup*" on page 5-44 of *Chapter 5, Integrated Services Digital Network (ISDN)*.

   Set the ISDN call profile appropriate for the ISDN service provider. The default profile is the ETSI specification for European Union (EU) countries (ETB for Basic Rate interfaces or ETP for Primary Rate interfaces). To use the Australian Telecom profile, for example, on Basic Rate interface BRI 0 for router HO1 and RG1, use the following command on each router:

   ```
   SET Q931=BRI0 PROFILE=AUS
   ```

   On the Head Office router, create a call to the Region 1 router:

   ```
   ADD ISDN CALL=Region1 OUTSUB=LOCAL SEARCHSUB=LOCAL PREC=IN
      NUMBER=1234567
   ```

   On the Region 1 router create a call to the Head Office router:

   ```
   ADD ISDN CALL=Region1 OUTSUB=LOCAL SEARCHSUB=LOCAL
      PREC=OUT NUMBER=9876543
   ```

2. **Set up the synchronous interfaces.**

   The synchronous interfaces on both routers must be set to the same speed as the leased line. For example, for a 9600 baud leased line, the synchronous interfaces must be set to 9600 baud, using the following command on each router:

   ```
   SET SYN=0 SPEED=9600
   ```

The speed of the synchronous interface must be set to correctly match the actual speed of the WAN connection, otherwise the utilisation calculations will produce erroneous results.

3. **Create a PPP interface to use the ISDN calls.**

   Create the PPP interfaces to use a leased line and one ISDN channel, and set the thresholds for bandwidth on demand. On the Head Office router create a PPP interface:

```
CREATE PPP=0 OVER=SYN0
ADD PPP=0 OVER=ISDN-Region1 TYPE=DEMAND
SET PPP=0 UPRATE=80 DOWNRATE=20
```

   On the Region 1 router create a PPP interface:

```
CREATE PPP=0 OVER=SYN0
ADD PPP=0 OVER=ISDN-Region1 TYPE=DEMAND
SET PPP=0 UPRATE=80 DOWNRATE=20
```

4. **Configure IP.**

   Configure a routing module to use the PPP interfaces. It could be IPX, DECnet or bridging but for this example IP is used. Static routes must be defined with on-demand links because a routing protocol would keep a link up continuously. Configure IP at the Head Office router:

```
ADD IP INT=ppp0 IP=192.168.35.113 MASK=255.255.255.240
ADD IP ROUTE=192.168.35.96 INT=ppp0 NEXT=192.168.35.114
   MET=2
```

   Configure IP at the Region 1 router:

```
ADD IP INT=ppp0 IP=192.168.35.114 MASK=255.255.255.240
ADD IP ROUTE=192.168.35.0 INT=ppp0 NEXT=192.168.35.113
   MET=2
ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXT=192.168.35.113 MET=3
```

   For a more detailed example of configuring IP see "*Configuration Examples*" on page 8-35 of *Chapter 8, Internet Protocol (IP)*. The command:

```
ENABLE PPP=0 DEBUG=UTIL
```

   can be used to see what bandwidth utilisation is being reported and the average utilisation. All values are expressed in hexadecimal. The utilisation is measured every second.

Command Reference

This section describes the commands available on the router to configure and manage the Point-to-Point Protocol on the router. The Point-to-Point Protocol (PPP) can be used on synchronous links, ISDN calls (see *Chapter 5, Integrated Services Digital Network (ISDN)*), ACC calls (see *Chapter 18, Asynchronous Call Control*), MIOX circuits (see *Chapter 6, X.25*), L2TP calls (see *Chapter 27, Layer Two Tunnelling Protocol (L2TP)*) and TDM groups (see *Chapter 22, Time Division Multiplexing (TDM)*). PPP can be used on the router to carry IP, IPX, DECnet and AppleTalk routing protocols, bridged protocols, and compressed and/or encrypted data.

See "*Conventions*" on page lxvii of *Preface* in the front of this manual for details of the conventions used to describe command syntax. See *Appendix A, Messages* for a complete list of messages and their meanings.

ACTIVATE PPP

Syntax `ACTIVATE PPP=`*`ppp-interface`* `RXPKT=`*`hexstring`*

where:

- *ppp-interface* is the PPP interface number.
- *hexstring* is a string of hexadecimal characters.

Description This command creates and sends a PPP packet to the specified PPP interface as if the packet had been received from the lower layer interface, and is intended for diagnostic and testing purposes.

The RXPKT parameter specifies the PPP packet to create and send, as a string of hexadecimal characters. For detailed information about PPP packet formats, see RFC 1661, "*The Point-to-Point Protocol (PPP)*".

This command is intended for debugging purposes only, and should not be used during normal operation.

Examples To create and send an LCP packet requesting CHAP authentication to PPP interface 1, use the command:

```
ACTIVATE PPP=1 RXPKT=ff03c023012100090305c22305
```

ADD PPP

Syntax

```
ADD PPP=ppp-interface OVER=physical-interface
   [AUTHENTICATION={CHAP|EITHER|PAP|NONE}] [AUTHMODE={IN|
   OUT|INOUT}] [CBDELAY=1..100] [CBMODE={ACCEPT|OFF|
   REQUEST}] [CBNUMBER=e164number]
   [CBOPERATION={E164NUMBER|USERAUTH}]
   [COMPALGORITHM={PREDICTOR|STACLZS}] [COMPRESSION={LINK|
   OFF}] [CONFIGURE={value|CONTINUOUS}] [LQR={ON|OFF|
   time}] [MAGIC={ON|OFF}] [MODEM={ON|OFF}]
   [NUMBER=number] [PREDCHECK={CRC16|CRCCCITT}]
   [RESTART=time] [STACCHECK={LCB|SEQUENCE}]
   [TERMINATE={value|CONTINUOUS}] [TYPE={DEMAND|PRIMARY|
   SECONDARY}]
```

where:

- *ppp-interface* is the PPP interface number.
- *physical-interface* is SYN*n*, ISDN-*callname*, ACC-*callname*, MIOX*n-circuitname*, TNL-*callname* or TDM-*groupname*.
- *e164number* is the phone number to dial when performing callback. It may contain digits (0–9) and should be a valid phone number as described in CCITT standard E.164.
- *value* is a retry threshold.
- *time* is a timer value in seconds.
- *number* is the number of PPP interfaces to add.

Description This command adds a synchronous port, an ISDN call, an ACC call, a MIOX circuit, an L2TP call or a TDM group to the PPP interface to use as a physical layer. The OVER parameter specifies the physical interface over which the PPP interface will run.

The AUTHENTICATION parameter specifies the authentication protocol to be used on the physical interface or channel. If CHAP is specified, the Challenge-Handshake Authentication Protocol (CHAP) is used. If PAP is specified, the Password Authentication Protocol (PAP) is used. If EITHER is specified, the router uses the option negotiation process to negotiate the authentication protocol to be used with the device at the remote end of the link, specifying CHAP as the first choice. If NONE is specified, no authentication protocol is used. The default is NONE.

The AUTHMODE parameter specifies how authentication requests to peers are affected by the direction of the ISDN or ACC call. The AUTHMODE parameter is only valid when the AUTHENTICATION parameter is set to a value other than NONE and the physical interface is an ISDN or ACC call. If IN is specified, authentication will only be requested for incoming calls from peers. If OUT is specified, authentication will only be requested for outgoing calls to peers. If INOUT is specified, authentication will always be requested regardless of the direction of the call. The default is INOUT.

The CBDELAY parameter specifies the delay, in tenths of a second, between bringing down a call for callback and actually making the call back to the peer. This parameter is used to handle the different timing requirements of various ISDN switches and is only valid for PPP links over ISDN calls and when the callback mode is REQUEST. The default is 1.

The CBMODE parameter specifies whether a callback request will be made or accepted during the LCP negotiation. If REQUEST is specified a request will be made for callback. If ACCEPT is specified requests for callback received from the peer will be accepted and processed, however AUTHENTICATION must be set to PAP or CHAP. If OFF is specified no callback requests will be made and callback requests will not be accepted. The default is OFF.

The CBNUMBER parameter specifies the number to include when requesting a callback with the CBOPERATION parameter set to E164NUMBER. The number specified should be a phone number as specified in the E.164 standard.

The CBOPERATION parameter specifies the callback operation to be included in the callback request to specify to the peer how to determine the callback number. If USERAUTH is specified the peer will use the username and password supplied during authentication to look up the callback number. If E164NUMBER is specified the callback number specified by the CBNUMBER parameter is included in the callback request. The default is USERAUTH.

The COMPALGORITHM parameter specifies the compression algorithm to use when compressing and decompressing PPP packets. If PREDICTOR is specified the Predictor algorithm will be used with type 1 encapsulation as specified in RFC 1978. If STACLZS is specified the Stac LZS algorithm will be used as specified in RFC 1974. The default is STACLZS.

The COMPRESSION parameter enables compression for the physical interface being added. The default is OFF. The LINK option should only be used when compression is required on the interface being added and not on others. For example, if a PPP multilink uses a compressing modem link and a normal dedicated leased line, COMPRESSION should be set to OFF on the physical interface to which the modem is connected, and LINK for the physical interface to

which the dedicated leased line is connected. If compression is required on all physical interfaces of a PPP interface, compression should be enabled by setting the COMPRESSION parameter to ON in the CREATE PPP or SET PPP command.

The CONFIGURE parameter sets the number of configure requests sent before some action is taken. For the LCP the action is to reset the hardware and start again. For all other protocols the action is to give up. The default is CONTINUOUS, which means that requests will be sent continuously.

The LQR parameter sets the LQR timer. If ON is specified, LQR is enabled with a default timer of 60 seconds. If a time is specified, LQR is enabled with the timer set to the specified time. If OFF is specified, LQR is disabled. The default is ON.

The MAGIC parameter enables or disables negotiation of the magic number option. The default is ON. The magic number is used to determine if a interface is looped back. The interface will not reach the OPENED state if there is a loopback.

The MODEM parameter specifies the state of synchronous modem control. The default is OFF. If ON is specified, the router will manipulate the DTR signal to trigger the modem to make a call whenever there is traffic (IDLE=ON) or when a backup link is required (TYPE=SECONDARY). Raising DTR to the modem triggers the modem to initiate a call to the modem at the other end of the link and enter data transfer mode. The router will keep the DTR signal to the modem raised, and will respond to the modem raising the DSR signal by activating the PPP interface. This parameter is only valid when the OVER parameter specifies a synchronous interface.

The NUMBER parameter specifies the number of physical interfaces to be added. This parameter is only valid when the OVER parameter specifies an ISDN call as the physical interface. The default is 1.

The PREDCHECK parameter specifies the type of CRC to be used for Predictor compression. The Predictor RFC specifies using CRC-16, however some router manufacturers have implemented Predictor with CRC-CCITT which is the CRC specified in RFC 1662, “PPP in HDLC-link Framing”. This value is not negotiated so the same value needs to be configured at both ends of the link for Predictor compression to work correctly.

The RESTART parameter specifies the time between successive retransmissions of unacknowledged configure requests or terminate requests. The default is 3 seconds.

The STACCHECK parameter specifies the check mode to used for the Stac LZS compression algorithm. If SEQUENCE is specified an incrementing sequence number is used to determine whether a packet has been lost and therefore whether the compression history needs to be reset. If LCB is specified an LCB value is used to determine if an error has occurred in a packet. The default is SEQUENCE.

The TERMINATE parameter sets the number of terminate requests sent when trying to close a link before it is assumed the link is down. The default is 2. The CONTINUOUS option specifies that requests will be sent continuously.

The TYPE parameter specifies the role of the physical interface for bandwidth on demand and leased line backup. The default is PRIMARY. If PRIMARY is specified, the link will be kept open all the time (IDLE=OFF) or opened when-

ever there is traffic (IDLE=ON). If SECONDARY is specified, the link will be opened only when the associated primary link fails. If DEMAND is specified, the link will be opened only when additional bandwidth is required.

To configure bandwidth on demand the ISDN channels are given a TYPE of DEMAND when they are added to the PPP interface. Adding one channel with a type of PRIMARY and other channels with a TYPE of DEMAND will ensure that there is always one channel available. If all channels are assigned a TYPE of DEMAND then there will be no channels open when there is no traffic, some traffic will cause one channel to be opened and continuous traffic will cause other channels to be opened. If there is one channel remaining opened then the IDLE timer is used to determine when this channel should be closed. For bandwidth on demand the IDLE timer should not be set to OFF.

To configure leased line backup the synchronous link is assigned a TYPE of PRIMARY and the ISDN call is assigned a TYPE of SECONDARY. When the primary link fails, LQR detects the failure and resets the link causing configure requests to be transmitted. If the primary link fails to reach the OPENED state after a number of configure request packets have been transmitted, the secondary link is activated. The number of configure request packets transmitted and the interval between successive retransmissions of configure request packets is controlled by the CONFIGURE and RESTART parameters. The CONFIGURE parameter needs to be specified as the default is CONTINUOUS. The time interval between link failure and activation of the secondary link depends on the LQR timer, and the CONFIGURE and RESTART parameters.

Examples To add synchronous interface 2 as an additional physical interface to PPP interface 1, and enable STAC LZS compression on the synchronous link with a check mode of LCB, use the command:

```
ADD PPP=1 OVER=SYN2 COMP=LINK STACCHECK=LCB
```

See Also CREATE PPP
DELETE PPP
DESTROY PPP
SET PPP
SHOW PPP

CREATE PPP

Syntax

```
CREATE PPP=ppp-interface OVER=physical-interface
   [AUTHENTICATION={CHAP|EITHER|PAP|NONE}] [AUTHMODE={IN|
   OUT|INOUT}] [BAP={ON|OFF}] [BAPMODE={CALL|CALLBACK}]
   [CBDELAY=1..100] [CBMODE={ACCEPT|OFF|REQUEST}]
   [CBNUMBER=e164number] [CBOPERATION={E164NUMBER|
   USERAUTH}] [COMPALGORITHM={PREDICTOR|STACLZS}]
   [COMPRESSION={ON|OFF|LINK}] [CONFIGURE={value|
   CONTINUOUS}] [DEBUGMAXBYTES=16..256]
   [DESCRIPTION=description] [DOWNRATE=0..100]
   [DOWNTIME=time] [ECHO={ON|OFF|period}] [ENCRYPTION={ON|
   OFF}] [FRAGMENT={ON|OFF}] [FRAGOVERHEAD=0.100]
   [IDLE={ON|OFF|time}] [IPREQUEST={ON|OFF}] [LQR={ON|OFF|
   time}] [MAGIC={ON|OFF}] [MODEM={ON|OFF}]
   [NULLFRAGTIMER=time] [NUMBER=number]
   [PASSWORD=password] [PREDCHECK={CRC16|CRCCCITT}]
   [RESTART=time] [STACCHECK={LCB|SEQUENCE}]
   [STARENTITY=1..255] [TERMINATE={value|CONTINUOUS}]
   [TYPE={DEMAND|PRIMARY|SECONDARY}] [UPRATE=0..100]
   [UPTIME=time] [USERNAME=username]
```

where:

- *ppp-interface* is the PPP interface number.
- *physical-interface* is SYN*n*, ISDN-*callname*, ACC-*callname*, MIOX*n-circuitname*, TNL-*callname* or TDM-*groupname*.
- *e164number* is the phone number to dial when performing callback. It may contain digits (0–9) and should be a valid phone number as described in CCITT standard E.164.
- *value* is a retry threshold.
- *description* is a character string, 1 to 70 characters in length. Valid characters are any printable character.
- *time* is a timer value in seconds.
- *period* is a decimal number in the range 1 to 4294967295.
- *number* is the number of PPP interfaces to create.
- *password* is the password to use for authentication, 1 to 32 characters in length. It may contain any printable character, and is case sensitive.
- *username* is the username to use for authentication, 1 to 32 characters in length. It may contain any printable character, and is case sensitive.

Description

This command creates the specified PPP interface running over a synchronous port, an ISDN call, an ACC call, a MIOX circuit, an L2TP call or a TDM group (referred to as a physical layer).

The OVER parameter specifies the physical interface over which the PPP interface will run. Additional physical interfaces can be added to the PPP interface using the ADD PPP command.

The AUTHENTICATION parameter specifies the authentication protocol to be used on the physical interface or channel. If CHAP is specified, the Challenge-Handshake Authentication Protocol (CHAP) is used. If PAP is specified, the Password Authentication Protocol (PAP) is used. If EITHER is specified, the router uses the option negotiation process to negotiate the authentication pro-

tocol to be used with the device at the remote end of the link, specifying CHAP as the first choice. If NONE is specified, no authentication protocol is used. The default is NONE.

The AUTHMODE parameter specifies how authentication requests to peers are affected by the direction of the ISDN or ACC call. The AUTHMODE parameter is only valid when the AUTHENTICATION parameter is set to a value other than NONE and the physical interface is an ISDN or ACC call. If IN is specified, authentication will only be requested for incoming calls from peers. If OUT is specified, authentication will only be requested for outgoing calls to peers. If INOUT is specified, authentication will always be requested regardless of the direction of the call. The default is INOUT.

The BAP parameter specifies whether or not the Bandwidth Allocation Protocol will be used for negotiating the activation of demand PPP links. The default is ON.

The BAPMODE parameter specifies which peer originates another link to add to the multilink bundle. For CALLBACK mode, the number to call must be configured on the call at the lower layer (ISDN, ACC or L2TP). The default is CALL.

The CBDELAY parameter specifies the delay, in tenths of a second, between bringing down a call for callback and actually making the call back to the peer. This parameter is used to handle the different timing requirements of various ISDN switches and is only valid for PPP links over ISDN calls and when the callback mode is REQUEST. The default is 1.

The CBMODE parameter specifies whether a callback request will be made or accepted during the LCP negotiation. If REQUEST is specified a request will be made for callback. If ACCEPT is specified requests for callback received from the peer will be accepted and processed, however AUTHENTICATION must be set to PAP or CHAP. If OFF is specified no callback requests will be made and callback requests will not be accepted. The default is OFF.

The CBNUMBER parameter specifies the number to include when requesting a callback with the CBOPERATION parameter set to E164NUMBER. The number specified should be a phone number as specified in the E.164 standard.

The CBOPERATION parameter specifies the callback operation to be included in the callback request to specify to the peer how to determine the callback number. If USERAUTH is specified the peer will use the username and password supplied during authentication to look up the callback number. If E164NUMBER is specified the callback number specified by the CBNUMBER parameter is included in the callback request. The default is USERAUTH.

The COMPALGORITHM parameter specifies the compression algorithm to use when compressing and decompressing PPP packets. If PREDICTOR is specified the Predictor algorithm will be used with type 1 encapsulation as specified in RFC 1978. If STACLZS is specified the Stac LZS algorithm will be used as specified in RFC 1974. The default is STACLZS.

The COMPRESSION parameter enables or disables the use of compression for the interface. When used with multilink, setting COMPRESSION to ON will compress the packets before they are sent to the individual links. Setting COMPRESSION to LINK will enable compression for the link specified by the OVER parameter. The default is OFF. The LINK option should only be used when compression is required on some physical interfaces and not on others. For example, if a PPP multilink uses a compressing modem link and a normal ded-

icated leased line, COMPRESSION should be set to OFF on the physical interface to which the modem is connected, and LINK for the physical interface to which the dedicated leased line is connected. If compression is required on all physical interfaces of a PPP interface, the COMPRESSION parameter should be set to ON.

The CONFIGURE parameter sets the number of configure requests sent before some action is taken. For the LCP the action is to reset the hardware and start again. For all other protocols the action is to give up. The default is CONTINUOUS, which means that requests will be sent continuously.

The DEBUGMAXBYTES parameter specifies the maximum number of bytes that are displayed for each packet when the PACKET debug option is enabled. The default is 32.

The DESCRIPTION parameter specifies a user-defined description for the interface, to make it easier to distinguish between a number of PPP interfaces.

The DOWNTIME parameter specifies the time, in seconds, that the PPP interface must have a total utilisation (as a percentage) below the threshold specified by the DOWNRATE parameter, before a channel is closed. The default is 60 for DOWNTIME and 20 for DOWNRATE. The UPRATE, UPTIME, DOWNRATE and DOWNTIME parameters are used in conjunction with the TYPE parameter to configure bandwidth on demand.

The ECHO parameter specifies whether or not LCP *Echo Request* and *Echo Reply* messages are used to determine link quality. If three consecutive *Echo Request* messages are transmitted without receiving an *Echo Reply* response, the link is deemed to be down. The ECHO and LQR parameters are mutually exclusive. If ECHO is enabled, LQR will be disabled. If LQR is enabled, ECHO will be set to OFF. If OFF is specified, *Echo Request* messages will not be transmitted. If ON is specified, *Echo Request* messages will be transmitted every 60 seconds. If a period in seconds is specified, *Echo Request* messages are transmitted at the specified interval.

The ENCRYPTION parameter enables or disables the use of encryption for the interface. The default is OFF.

The FRAGMENT parameter applies only to a multilink bundle interface, and determines whether packets are fragmented or not. The default is OFF. Fragmentation must be disabled if compression is required.

The FRAGOVERHEAD parameter specifies the maximum allowable overhead, as a percentage, for fragmenting packets using the variable fragmentation scheme for multilink PPP. If this limit will be exceeded for any packet the packet is fragmented using the fixed fragmentation scheme. The default is 5. The variable fragmentation scheme spreads the packet over all the links in the multilink bundle by splitting the packet into variable sized fragments to match the speed of individual links. Larger fragments are transmitted over faster links, thereby providing an inherent load balancing scheme. The fixed fragmentation scheme spreads the packet over all the links in the multilink bundle by splitting the packet into equal fixed sized fragments. If the number of links is large and the packet is relatively small a fragment is not transmitted over every link.

The IDLE parameter controls the dial-on-demand feature. If ON is specified, dial-on-demand is enabled with a default timer of 60 seconds. If a time is specified, dial-on-demand is enabled with the timer set to the specified time. If OFF is specified, dial-on-demand is disabled. When the dial-on-demand feature is

activated, PPP brings up the link when there is traffic to be sent, and takes down the link when there has been no traffic for the specified timer period. The effect on a PPP interface using an ISDN call will be to connect the call when traffic is to be sent and disconnect the call when no traffic has been sent or received for the specified timer period. For other physical interfaces, this parameter has no effect, as the links are always connected. The default is OFF.

The IPREQUEST parameter specifies whether or not a request will be made for an IP address to be allocated by the peer during the IPCP negotiation. If ON is specified a request will be made. If OFF is specified a request will not be specified. The default is OFF.

The LQR parameter sets the LQR timer. If ON is specified, LQR is enabled with a default timer of 60 seconds. If a time is specified, LQR is enabled with the timer set to the specified time. If OFF is specified, LQR is disabled. The default is ON.

The MAGIC parameter enables or disables negotiation of the magic number option. The default is ON. The magic number is used to determine if a interface is looped back. The interface will not reach the OPENED state if there is a loopback.

The MODEM parameter specifies the state of synchronous modem control. The default is OFF. If ON is specified, the router will manipulate the DTR signal to trigger the modem to make a call whenever there is traffic (IDLE=ON) or when a backup link is required (TYPE=SECONDARY). Raising DTR to the modem triggers the modem to initiate a call to the modem at the other end of the link and enter data transfer mode. The router will keep the DTR signal to the modem raised, and will respond to the modem raising the DSR signal by activating the PPP interface. This parameter is only valid when the OVER parameter specifies a synchronous interface.

The NUMBER parameter specifies the number of physical interfaces to be created. This parameter is only valid when the OVER parameter specifies an ISDN call as the physical interface. The default is 1.

The NULLFRAGTIMER parameter specifies the maximum time, in seconds, a link in a multilink bundle may be idle before a NULL fragment is transmitted over the link. NULL fragments are used to keep the last sequence number transmitted over the link up to date. The default is 3.

The PASSWORD parameter specifies the password to use when the peer requests authentication using either CHAP or PAP. This is normally required for network lines between routers, for which an authentication protocol has been selected with the AUTHENTICATION parameter.

The PREDCHECK parameter specifies the type of CRC to be used for Predictor compression. The Predictor RFC specifies using CRC-16, however some router manufacturers have implemented Predictor with CRC-CCITT which is the CRC specified in RFC 1662, “PPP in HDLC-link Framing”. This value is not negotiated so the same value needs to be configured at both ends of the link for Predictor compression to work correctly.

The RESTART parameter specifies the time between successive retransmissions of unacknowledged configure requests or terminate requests. The default is 3 seconds.

The STACCHECK parameter specifies the check mode to used for the Stac LZS compression algorithm. If SEQUENCE is specified an incrementing sequence

number is used to determine whether a packet has been lost and therefore whether the compression history needs to be reset. If LCB is specified an LCB value is used to determine if an error has occurred in a packet. The default is SEQUENCE.

The STARENTITY parameter specifies the star entity and the encryption algorithm to be used by the encryption channel configured by the PPP interface. This parameter must be specified if PPP encryption is enabled.

The TERMINATE parameter sets the number of terminate requests sent when trying to close a link before it is assumed the link is down. The default is 2. The CONTINUOUS option specifies that requests will be sent continuously.

The TYPE parameter specifies the role of the physical interface for bandwidth on demand and leased line backup. The default is PRIMARY. If PRIMARY is specified, the link will be kept open all the time (IDLE=OFF) or opened whenever there is traffic (IDLE=ON). If SECONDARY is specified, the link will be opened only when the associated primary link fails. If DEMAND is specified, the link will be opened only when the additional bandwidth is required.

To configure bandwidth on demand the ISDN channels are given a TYPE of DEMAND when they are added to the PPP interface. Adding one channel with a type of PRIMARY and other channels with a TYPE of DEMAND will ensure that there is always one channel available. If all channels are assigned a TYPE of DEMAND then there will be no channels open when there is no traffic, some traffic will cause one channel to be opened and continuous traffic will cause other channels to be opened. If there is one channel remaining opened then the IDLE timer is used to determine when this channel should be closed. In this case it is recommended that the IDLE timer not be set to OFF.

To configure leased line backup the synchronous link is assigned a TYPE of PRIMARY and the ISDN call is assigned a TYPE of SECONDARY. When the primary link fails, LQR detects the failure and resets the link causing configure requests to be transmitted. If the primary link fails to reach the OPENED state after a number of configure request packets have been transmitted, the secondary link is activated. The number of configure request packets transmitted and the interval between successive retransmissions of configure request packets is controlled by the CONFIGURE and RESTART parameters. The CONFIGURE parameter needs to be specified as the default is CONTINUOUS. The time interval between link failure and activation of the secondary link depends on the LQR timer, and the CONFIGURE and RESTART parameters.

The UPTIME parameter specifies the time, in seconds, that the PPP interface must have a total utilisation (as a percentage) above the threshold specified by the UPRATE parameter, before an additional channel is opened. The default is 30 for UPTIME and 80 for UPRATE. The UPRATE, UPTIME, DOWNRATE and DOWNTIME parameters are used in conjunction with the TYPE parameter to configure bandwidth on demand.

The USERNAME parameter specifies the username to be used when generating PAP authentication requests and when responding to CHAP authentication challenges. If the USERNAME is not set the router's system name will be used by default.

For security reasons this command will only be accepted if the user has SECURITY OFFICER privilege.

Examples To create PPP interface 0 with two on-demand channels over the ISDN call "ISDN-Region1", use the command:

```
CREATE PPP=0 OVER=ISDN-Region1 IDLE=ON NUM=2 TYPE=DEMAND
```

See Also ADD PPP
DELETE PPP
DESTROY PPP
DISABLE PPP
ENABLE PPP
RESET PPP
SET PPP
SHOW PPP

CREATE PPP TEMPLATE

Syntax

```
CREATE PPP TEMPLATE=template [COPY=template]
   [AUTHENTICATION={CHAP|EITHER|PAP|NONE}] [BAP={ON|OFF}]
   [BAPMODE={CALL|CALLBACK}] [CBDELAY=1..100]
   [CBMODE={ACCEPT|OFF|REQUEST}] [CBNUMBER=e164number]
   [CBOPERATION={E164NUMBER|USERAUTH}]
   [COMPALGORITHM={PREDICTOR|STACLZS}] [COMPRESSION={ON|
   OFF|LINK}] [DEBUGMAXBYTES=16..256]
   [DESCRIPTION=description] [ECHO={ON|OFF|period}]
   [ENCRYPTION={ON|OFF}] [FRAGMENT={ON|OFF}]
   [FRAGOVERHEAD=0..100] [IDLE={ON|OFF|time}]
   [IPREQUEST={ON|OFF}] [LOGIN={ALL|RADIUS|TACACS|USER}]
   [LQR={ON|OFF|time}] [MAGIC={ON|OFF}] [MAXLINKS=1..64]
   [NULLFRAGTIMER=time] [PASSWORD=password]
   [PREDCHECK={CRC16|CRCCCITT}] [RESTART=time]
   [STACCHECK={LCB|SEQUENCE}] [STARENTITY=1..255]
   [USERNAME=username]
```

where:

- *template* is a number in the range 0 to 31.
- *e164number* is the phone number to dial when performing callback. It may contain digits (0–9) and should be a valid phone number as described in CCITT standard E.164.
- *description* is a character string, 1 to 70 characters in length. Valid characters are any printable character.
- *period* is a decimal number in the range 1 to 4294967295.
- *time* is a timer value in seconds.
- *password* is the password to use for authentication, 1 to 32 characters in length. It may contain any printable character, and is case sensitive.
- *username* is the username to use for authentication, 1 to 32 characters in length. It may contain any printable character, and is case sensitive.

Description This command creates a PPP template that is used to configure dynamic PPP interfaces that are created when an ISDN, ACC or L2TP call is activated.

The TEMPLATE parameter specifies the number of the template to create. The specified template must not already exist.

The AUTHENTICATION parameter specifies the authentication protocol to be used on the physical interface or channel. If CHAP is specified, the Challenge-Handshake Authentication Protocol (CHAP) is used. If PAP is specified, the Password Authentication Protocol (PAP) is used. If EITHER is specified, the router uses the option negotiation process to negotiate the authentication protocol to be used with the device at the remote end of the link, specifying CHAP as the first choice. If NONE is specified, no authentication protocol is used. The default is NONE.

The BAP parameter specifies whether or not the Bandwidth Allocation Protocol will be used for negotiating the activation of demand PPP links. The default is ON.

The BAPMODE parameter specifies which peer originates another link to add to the multilink bundle. For CALLBACK mode, the number to call must be configured on the call at the lower layer (ISDN, ACC or L2TP). The default is CALL.

The CBDELAY parameter specifies the delay, in tenths of a second, between bringing down a call for callback and actually making the call back to the peer. This parameter is used to handle the different timing requirements of various ISDN switches and is only valid for PPP links over ISDN calls and when the callback mode is REQUEST. The default is 1.

The CBMODE parameter specifies whether a callback request will be made or accepted during the LCP negotiation. If REQUEST is specified a request will be made for callback. If ACCEPT is specified requests for callback received from the peer will be accepted and processed, however AUTHENTICATION must be set to PAP or CHAP. If OFF is specified no callback requests will be made and callback requests will not be accepted. The default is OFF.

The CBNUMBER parameter specifies the number to include when requesting a callback with the CBOPERATION parameter set to E164NUMBER. The number specified should be a phone number as specified in the E.164 standard.

The CBOPERATION parameter specifies the callback operation to be included in the callback request to specify to the peer how to determine the callback number. If USERAUTH is specified the peer will use the username and password supplied during authentication to look up the callback number. If E164NUMBER is specified the callback number specified by the CBNUMBER parameter is included in the callback request. The default is USERAUTH.

The COMPALGORITHM parameter specifies the compression algorithm to use when compressing and decompressing PPP packets. If PREDICTOR is specified the Predictor algorithm will be used with type 1 encapsulation as specified in RFC 1978. If STACLZS is specified the Stac LZS algorithm will be used as specified in RFC 1974. The default is STACLZS.

The COMPRESSION parameter enables or disables the use of compression for the interface. When used with multilink, setting COMPRESSION to ON will compress the packets before they are sent to the individual links. Setting COMPRESSION to LINK will enable compression for the link specified by the OVER parameter. The default is OFF. The LINK option should only be used when compression is required on some physical interfaces and not on others. For example, if a PPP multilink uses a compressing modem link and a normal dedicated leased line, COMPRESSION should be set to OFF on the physical interface to which the modem is connected, and LINK for the physical interface to which the dedicated leased line is connected. If compression is required on all

physical interfaces of a PPP interface, the COMPRESSION parameter should be set to ON.

The COPY parameter specifies the name of an existing template to copy as the default values for this template. Any other parameters modify the copy.

The DEBUGMAXBYTES parameter specifies the maximum number of bytes that are displayed for each packet when the PACKET debug option is enabled. The default is 32.

The DESCRIPTION parameter specifies a user-defined description for the interface, to make it easier to distinguish between a number of PPP interfaces.

The ECHO parameter specifies whether or not LCP *Echo Request* and *Echo Reply* messages are used to determine link quality. If three consecutive *Echo Request* messages are transmitted without receiving an *Echo Reply* response, the link is deemed to be down. The ECHO and LQR parameters are mutually exclusive. If ECHO is enabled, LQR will be disabled. If LQR is enabled, ECHO will be set to OFF. If OFF is specified, *Echo Request* messages will not be transmitted. If ON is specified, *Echo Request* messages will be transmitted every 60 seconds. If a period in seconds is specified, *Echo Request* messages are transmitted at the specified interval.

The ENCRYPTION parameter enables or disables the use of encryption for the interface. The default is OFF.

The FRAGMENT parameter applies only to a multilink bundle interface, and determines whether packets are fragmented or not. The default is OFF. Fragmentation must be disabled if compression is required.

The FRAGOVERHEAD parameter specifies the maximum allowable overhead, as a percentage, for fragmenting packets using the variable fragmentation scheme for multilink PPP. If this limit will be exceeded for any packet the packet is fragmented using the fixed fragmentation scheme. The default is 5. The variable fragmentation scheme spreads the packet over all the links in the multilink bundle by splitting the packet into variable sized fragments to match the speed of individual links. Larger fragments are transmitted over faster links, thereby providing an inherent load balancing scheme. The fixed fragmentation scheme spreads the packet over all the links in the multilink bundle by splitting the packet into equal fixed sized fragments. If the number of links is large and the packet is relatively small a fragment is not transmitted over every link.

The IDLE parameter controls the dial-on-demand feature. If ON is specified, dial-on-demand is enabled with a default timer of 60 seconds. If a time is specified, dial-on-demand is enabled with the timer set to the specified time. If OFF is specified, dial-on-demand is disabled. When the dial-on-demand feature is activated, PPP brings up the link when there is traffic to be sent, and takes down the link when there has been no traffic for the specified timer period. The effect on a PPP interface using an ISDN call will be to connect the call when traffic is to be sent and disconnect the call when no traffic has been sent or received for the specified timer period. For other physical interfaces, this parameter has no effect, as the links are always connected. The default is OFF.

The IPREQUEST parameter specifies whether or not a request will be made for an IP address to be allocated by the peer during the IPCP negotiation. If ON is specified a request will be made. If OFF is specified a request will not be specified. The default is OFF.

The LOGIN parameter specifies which login procedure the call creating this dynamic interface must use when it is activated. If RADIUS is specified, the router will send requests to the configured RADIUS server(s) to authenticate the call. If TACACS is specified, the router will send requests to the configured TACACS server(s) to authenticate the call. If USER is specified, the router will check the User Authentication Database to authenticate the call. If ALL is specified, the router will try all methods to authenticate the call.

The LQR parameter sets the LQR timer. If ON is specified, LQR is enabled with a default timer of 60 seconds. If a time is specified, LQR is enabled with the timer set to the specified time. If OFF is specified, LQR is disabled. The default is ON.

The MAGIC parameter enables or disables negotiation of the magic number option. The default is ON. The magic number is used to determine if a interface is looped back. The interface will not reach the OPENED state if there is a loopback.

The MAXLINKS parameter specifies the maximum number of links allowed in a multilink PPP interface created using this template.

The NULLFRAGTIMER parameter specifies the maximum time, in seconds, a link in a multilink bundle may be idle before a NULL fragment is transmitted over the link. NULL fragments are used to keep the last sequence number transmitted over the link up to date. The default is 3.

The PASSWORD parameter specifies the password to use when the peer requests authentication using either CHAP or PAP. This is normally required for network lines between routers, for which an authentication protocol has been selected with the AUTHENTICATION parameter.

The PREDCHECK parameter specifies the type of CRC to be used for Predictor compression. The Predictor RFC specifies using CRC-16, however some router manufacturers have implemented Predictor with CRC-CCITT which is the CRC specified in RFC 1662, “PPP in HDLC-link Framing”. This value is not negotiated so the same value needs to be configured at both ends of the link for Predictor compression to work correctly.

The RESTART parameter specifies the time between successive retransmissions of unacknowledged configure requests or terminate requests. The default is 3 seconds.

The STACCHECK parameter specifies the check mode to used for the Stac LZS compression algorithm. If SEQUENCE is specified an incrementing sequence number is used to determine whether a packet has been lost and therefore whether the compression history needs to be reset. If LCB is specified an LCB value is used to determine if an error has occurred in a packet. The default is SEQUENCE.

The STARENTITY parameter specifies the star entity and the encryption algorithm to be used by the encryption channel configured by the PPP interface. This parameter must be specified if PPP encryption is enabled.

The USERNAME parameter specifies the username to be used when generating PAP authentication requests and when responding to CHAP authentication challenges. If the USERNAME is not set the router’s system name will be used by default.

For security reasons this command will only be accepted if the user has SECURITY OFFICER privilege.

Examples To create a template that creates a dynamic PPP interface with BAP and Predictor compression enabled, use the command:

```
CREATE PPP TEMPLATE=1 BAP=ON BAPMODE=CALL
   DESCRIPTION="Dynamic PPP with Predictor and BAP"
   COMPRESSION=ON COMPALGORITHM=PREDICTOR
```

To create PPP template pppT2 using the factory default settings, use the command:

```
CREATE PPP TEMPLATE=2
```

See Also DESTROY PPP TEMPLATE
DISABLE PPP TEMPLATE DEBUG
ENABLE PPP TEMPLATE DEBUG
SET PPP TEMPLATE
SHOW PPP TEMPLATE

DELETE PPP

Syntax

```
DELETE PPP=ppp-interface OVER=physical-interface
   [NUMBER=number] [TYPE={DEMAND|PRIMARY|SECONDARY}]
```

where:

- *ppp-interface* is the PPP interface number.
- *physical-interface* is SYN*n*, ISDN-*callname*, ACC-*callname*, MIOX*n-circuitname*, TNL-*callname* or TDM-*groupname*.
- *number* is the number of physical interfaces to delete.

Description This command deletes the specified synchronous port, ISDN call, ACC call, MIOX circuit, L2TP call or TDM group from use by a PPP interface as a physical layer. The interface may be left with no physical layers.

The OVER parameter specifies the physical interface to be deleted.

The NUMBER parameter specifies the number of physical interfaces to be deleted. This parameter is only valid when the OVER parameter specifies an ISDN call as the physical interface. The default is 1.

The TYPE parameter specifies the role of the physical interface for bandwidth on demand and leased line backup. The default is PRIMARY.

Examples To delete synchronous interface 2 as a physical interface from PPP interface 1, use the command:

```
DELETE PPP=1 OVER=SYN2
```

See Also ADD PPP
CREATE PPP
DESTROY PPP
DISABLE PPP
ENABLE PPP
RESET PPP
SET PPP
SHOW PPP

DESTROY PPP

Syntax `DESTROY PPP=`*`ppp-interface`*

where:

- *ppp-interface* is the PPP interface number.

Description This command destroys the specified PPP interface, as opposed to the DELETE PPP command which deletes a physical interface used by a PPP interface.

Examples To destroy PPP interface 0, use the command:

```
DESTROY PPP=0
```

See Also ADD PPP
CREATE PPP
DELETE PPP
DISABLE PPP
ENABLE PPP
RESET PPP
SET PPP
SHOW PPP

DESTROY PPP TEMPLATE

Syntax `DESTROY PPP TEMPLATE=`*`template`*

where:

- *template* is a number in the range 0 to 31.

Description This command destroys the specified PPP template and eliminates any call associations. The TEMPLATE parameter specifies the number of the template to destroy. The specified template must already exist.

Examples To destroy template 1, use the command:

```
DESTROY PPP TEMPLATE=1
```

See Also CREATE PPP TEMPLATE
DISABLE PPP TEMPLATE DEBUG
ENABLE PPP TEMPLATE DEBUG
SET PPP TEMPLATE
SHOW PPP TEMPLATE

DISABLE PPP

Syntax `DISABLE PPP=`*`ppp-interface`*

where:

- *ppp-interface* is the PPP interface number.

Description This command disables the specified PPP interface. The interface must currently be enabled. The interface is not available for use by higher layer network protocols, but the configuration is retained in nonvolatile storage and is restored when the interface is re-enabled.

Examples To disable PPP interface 2, use the command:

```
DISABLE PPP=2
```

See Also ADD PPP
CREATE PPP
DELETE PPP
DISABLE PPP
ENABLE PPP
RESET PPP
SET PPP
SHOW PPP

DISABLE PPP DEBUG

Syntax `DISABLE PPP=`*`ppp-interface`* `DEBUG={ALL|AUTH|BAPPKT|BAPSTATE|CALLBACK|DEMAND|ENCO|LCP|NCP|PKT|UTILISATION}[,...]`

where:

- *ppp-interface* is the PPP interface number.

Description This command disables the debugging option for the specified PPP interface. The option must currently be enabled. A list of options separated by commas may be specified to disable more than one debugging option at a time.

The DEBUG parameter specifies which debugging options are to be disabled. The value of this parameter is a single item or a comma-separated list of items. The items allowed and the debugging that results from specifying the item are shown in Table 3-6 on page 3-51.

Examples To disable all debugging options on PPP interface 2, use the command:

```
DISABLE PPP=2 DEBUG=ALL
```

See Also ENABLE PPP DEBUG

DISABLE PPP TEMPLATE DEBUG

Syntax

```
DISABLE PPP TEMPLATE=template DEBUG={ALL|AUTH|BAPPKT|
   BAPSTATE|CALLBACK|DEMAND|ENCO|LCP|NCP|PKT|
   UTILISATION}[,...]
```

where:

- *template* is a number in the range 0 to 31.

Description This command disables the debugging option for dynamic PPP interfaces created using the specified PPP template. A list of options separated by commas may be specified to disable more than one debugging option at a time.

The TEMPLATE parameter specifies the number of the template for which debugging is to be disabled. The specified template must already exist.

The DEBUG parameter specifies which debugging options are to be disabled. The value of this parameter is a single item or a comma-separated list of items. The items allowed and the debugging that results from specifying the item are shown in Table 3-6 on page 3-51.

Examples To disable the display of debugging information for dial on demand link activation on template 2, use the command:

```
DISABLE PPP TEMPLATE=2 DEBUG=DEMAND
```

See Also CREATE PPP TEMPLATE
DESTROY PPP TEMPLATE
ENABLE PPP TEMPLATE DEBUG
SET PPP TEMPLATE
SHOW PPP TEMPLATE

ENABLE PPP

Syntax

```
ENABLE PPP=ppp-interface
```

where:

- *ppp-interface* is the PPP interface number.

Description This command enables the specified PPP interface. The interface must currently be disabled. The interface configuration is restored to the settings in existence before the interface was disabled. The interface is made available to network layer protocols to transmit and receive data.

Examples To enable PPP interface 2, use the command:

```
ENABLE PPP=2
```

See Also ADD PPP
CREATE PPP
DELETE PPP
DESTROY PPP
DISABLE PPP
RESET PPP
SET PPP
SHOW PPP

ENABLE PPP DEBUG

Syntax

```
ENABLE PPP=ppp-interface DEBUG={ALL|AUTH|BAPPKT|BAPSTATE|
   CALLBACK|DEMAND|ENCO|LCP|NCP|PKT|UTILISATION}[,...]
   [PORT=port-number] [TIMEOUT={NONE|1..4000000000}]
   [NUMPKTS={CONT|1..4000000000}]
```

where:

- *ppp-interface* is the PPP interface number.
- *port-number* is the number of an asynchronous port on the router. Ports are numbered starting at zero (0).

Description This command enables the debugging option for the specified PPP interface. Debugging may or may not be enabled already. Debugging information is sent to the port or telnet session from which the command was entered if the PORT parameter was not specified, otherwise it is sent to the specified port. A list of options separated by commas may be specified to enable more than one debugging option at a time. For packet debugging, the number of packets output may be specified. For all other types of debugging, the length of time that debugging will continue may be specified.

The DEBUG parameter specifies which debugging options are to be disabled. The value of this parameter is a single item or a comma-separated list of items. The items allowed and the debugging that results from specifying the item are shown in Table 3-6 on page 3-51.

Table 3-6: Point-to-Point Protocol (PPP) debugging options.

Option	Description
ALL	All debug options.
AUTH	PPP authentication. If LCP opens on a link but the network protocols remain in the CLOSED state, the most likely cause is an authentication failure.
BAPPKT	BAP packets received over the interface.
BAPSTATE	BAP state machine transitions.
CALLBACK	Callback state machine transitions.
DEMAND	Packets that cause on-demand links to be activated.
ENCO	ENCO state machine used to control attachment to and detachment from the ENCO (encryption/compression) module.
LCP	LCP state machine transitions.
NCP	NCP state machine transitions.
PKT	All packets received and transmitted on the PPP interface.

Table 3-6: Point-to-Point Protocol (PPP) debugging options. (Continued)

Option	Description
UTILISATION	Utilisation measurements for each lower layer interface and the overall utilisation.

Enabling all debug options with ENABLE PPP DEBUG=ALL may generate enormous amounts of output, causing the router to lock up. Use the TIMEOUT or NUMPKTS options to limit the amount of output generated.

The PORT parameter specifies the asynchronous port to which the debug output is to be sent. This enables debugging to be enabled in a script. The default is to send the output to the terminal or Telnet session from which the command was executed. Each time the ENABLE PPP DEBUG command is entered the destination of the debugging output is calculated again using this rule.

The TIMEOUT parameter specifies a time in seconds after which debugging will automatically cease. If NONE is specified then debugging must be disabled manually. The timeout only applies to debugging modes which do not involve the output of data packets, that is, all debugging modes except for PKT. The value of the TIMEOUT parameter the first time an applicable debugging mode is enabled will be retained for future ENABLE PPP DEBUG commands. The default is NONE.

The NUMPKTS parameter specifies, for PKT debugging, the number of packets to be displayed before debugging ceases. This option is useful when attempting to debug a very busy link, since the amount of output generated by PKT debugging can easily cause the router to lock up the device to which the debugging output is being sent. The value of this parameter the first time PKT debugging is enabled will be retained for subsequent ENABLE PPP DEBUG commands. If CONT is specified, packet debugging will continue indefinitely and must be disabled manually. The default is CONT.

Examples To enable the display of debugging information for dial on demand link activation on PPP interface 2, use the command:

```
ENABLE PPP=2 DEBUG=DEMAND
```

See Also DISABLE PPP DEBUG

ENABLE PPP TEMPLATE DEBUG

Syntax

```
ENABLE PPP TEMPLATE=template DEBUG={ALL|AUTH|BAPPKT|
    BAPSTATE|CALLBACK|DEMAND|ENCO|LCP|NCP|PKT|
    UTILISATION}[,...] [PORT=port-number] [TIMEOUT={NONE|
    1..4000000000}] [NUMPKTS={CONT|1..4000000000}]
```

where:

- *template* is a number in the range 0 to 31.
- *port-number* is the number of an asynchronous port on the router. Ports are numbered starting at zero (0).

Description

This command enables the debugging option for dynamic PPP interfaces created using the specified PPP template. Debugging may or may not be enabled already. Debugging information is sent to the port or telnet session from which the command was entered if the PORT parameter was not specified, otherwise it is sent to the specified port. A list of options separated by commas may be specified to enable more than one debugging option at a time. For packet debugging, the number of packets output may be specified. For all other types of debugging, the length of time that debugging will continue may be specified.

The TEMPLATE parameter specifies the number of the template for which debugging is to be enabled. The specified template must already exist.

The DEBUG parameter specifies which debugging options are to be disabled. The value of this parameter is a single item or a comma-separated list of items. The items allowed and the debugging that results from specifying the item are shown in Table 3-6 on page 3-51.

Enabling all debug options with ENABLE PPP TEMPLATE DEBUG=ALL may generate enormous amounts of output, causing the router to lock up. Use the TIMEOUT or NUMPKTS options to limit the amount of output generated.

The PORT parameter specifies the asynchronous port to which the debug output is to be sent. This enables debugging to be enabled in a script. The default is to send the output to the terminal or Telnet session from which the command was executed. Each time the ENABLE PPP TEMPLATE DEBUG command is entered the destination of the debugging output is calculated again using this rule.

The TIMEOUT parameter specifies a time in seconds after which debugging will automatically cease. If NONE is specified then debugging must be disabled manually. The timeout only applies to debugging modes which do not involve the output of data packets, that is, all debugging modes except for PKT. The value of the TIMEOUT parameter the first time an applicable debugging mode is enabled will be retained for future ENABLE PPP TEMPLATE DEBUG commands. The default is NONE.

The NUMPKTS parameter specifies, for PKT debugging, the number of packets to be displayed before debugging ceases. This option is useful when attempting to debug a very busy link, since the amount of output generated by PKT debugging can easily cause the router to lock up the device to which the debugging output is being sent. The value of this parameter the first time PKT debugging is enabled will be retained for subsequent ENABLE PPP TEM-

PLATE DEBUG commands. If CONT is specified, packet debugging will continue indefinitely and must be disabled manually. The default is CONT.

Examples To enable the display of debugging information for dial on demand link activation on template 2, use the command:

```
ENABLE PPP TEMPLATE=2 DEBUG=DEMAND
```

See Also CREATE PPP TEMPLATE
DESTROY PPP TEMPLATE
DISABLE PPP TEMPLATE DEBUG
SET PPP TEMPLATE
SHOW PPP TEMPLATE

PURGE PPP

Syntax `PURGE PPP`

Description This command destroys all PPP interfaces and reinitialises the PPP module.

Examples To the PPP configuration, use the command:

```
PURGE PPP
```

See Also DELETE PPP
DESTROY PPP
DISABLE PPP
ENABLE PPP

RESET PPP

Syntax `RESET PPP=`*`ppp-interface`* `[COUNTERS]`

where:

- *ppp-interface* is the PPP interface number.

Description This command resets the specified PPP interface, or the counters for the specified PPP interface.

If the COUNTERS parameter is not specified, the interface is reset, forcing the interface to renegotiate all protocols and options. If the COUNTERS parameter is specified, all counters for the interface are reset to zero (0).

Examples To reset PPP interface 0, use the command:

```
RESET PPP=0
```

To reset all counters for PPP interface 0 without resetting the interface itself, use the command:

```
RESET PPP=0 COUNTERS
```

See Also DELETE PPP
DESTROY PPP
DISABLE PPP
ENABLE PPP
PURGE PPP

SET PPP

Syntax

```
SET PPP[=ppp-interface] [OVER=physical-interface]
   [AUTHENTICATION={CHAP|EITHER|PAP|NONE}] [AUTHMODE={IN|
   OUT|INOUT}] [BAP={ON|OFF}] [BAPMODE={CALL|CALLBACK}]
   [CBDELAY=1..100] [CBMODE={ACCEPT|OFF|REQUEST}]
   [CBNUMBER=e164number] [CBOPERATION={E164NUMBER|
   USERAUTH}] [COMPALGORITHM={PREDICTOR|STACLZS}]
   [COMPRESSION={ON|OFF|LINK}] [CONFIGURE={value|
   CONTINUOUS}] [DEBUGMAXBYTES=16..256]
   [DESCRIPTION=description] [DNSPRIMARY=ipadd]
   [DNSSECONDARY=ipadd] [DOWNRATE=0..100] [DOWNTIME=time]
   [ECHO={ON|OFF|period}] [ENCRYPTION={ON|OFF}]
   [FRAGMENT={ON|OFF}] [FRAGOVERHEAD=0.100] [IDLE={ON|OFF|
   time}] [IPREQUEST={ON|OFF}] [LQR={ON|OFF|time}]
   [MAGIC={ON|OFF}] [MODEM={ON|OFF}] [NULLFRAGTIMER=time]
   [NUMBER=number] [PASSWORD=password] [PREDCHECK={CRC16|
   CRCCCITT}] [RESTART=time] [STACCHECK={LCB|SEQUENCE}]
   [STARENTITY=1..255] [TERMINATE={value|CONTINUOUS}]
   [TYPE={DEMAND|PRIMARY|SECONDARY}] [UPRATE=0..100]
   [UPTIME=time] [USERNAME=username] [WINSPRIMARY=ipadd]
   [WINSSECONDARY=ipadd]
```

where:

- *ppp-interface* is the PPP interface number.
- *physical-interface* is SYN*n*, ISDN-*callname*, ACC-*callname*, MIOX*n-circuitname*, TNL-*callname* or TDM-*groupname*.
- *e164number* is the phone number to dial when performing callback. It may contain digits (0–9) and should be a valid phone number as described in CCITT standard E.164.
- *value* is a retry threshold.
- *ipadd* is an IP address in dotted decimal notation.
- *description* is a character string, 1 to 70 characters in length. Valid characters are any printable character.
- *time* is a timer value in seconds.
- *period* is a decimal number in the range 1 to 4294967295.
- *number* is the number of PPP interfaces to create.
- *password* is the password to use for authentication, 1 to 32 characters in length. It may contain any printable character, and is case sensitive.
- *username* is the username to use for authentication, 1 to 32 characters in length. It may contain any printable character, and is case sensitive.

Description This command is used to change the configuration parameters of a PPP interface running over a synchronous port, an ISDN call, an ACC call, a MIOX circuit, an L2TP call or a TDM group (referred to as a physical layer). It is also used to set global primary and secondary DNS and WINS server addresses. In this case the PPP interface may not be specified. All other options require the PPP interface to be specified.

The OVER parameter specifies the physical interface over which the PPP interface is running.

The AUTHENTICATION parameter specifies the authentication protocol to be used on the physical interface or channel. If CHAP is specified, the Challenge-Handshake Authentication Protocol (CHAP) is used. If PAP is specified, the Password Authentication Protocol (PAP) is used. If EITHER is specified, the router uses the option negotiation process to negotiate the authentication protocol to be used with the device at the remote end of the link, specifying CHAP as the first choice. If NONE is specified, no authentication protocol is used. The default is NONE.

The AUTHMODE parameter specifies how authentication requests to peers are affected by the direction of the ISDN or ACC call. The AUTHMODE parameter is only valid when the AUTHENTICATION parameter is set to a value other than NONE and the physical interface is an ISDN or ACC call. If IN is specified, authentication will only be requested for incoming calls from peers. If OUT is specified, authentication will only be requested for outgoing calls to peers. If INOUT is specified, authentication will always be requested regardless of the direction of the call. The default is INOUT.

The BAP parameter specifies whether or not the Bandwidth Allocation Protocol will be used for negotiating the activation of demand PPP links. The default is ON.

The BAPMODE parameter specifies which peer originates another link to add to the multilink bundle. For CALLBACK mode, the number to call must be configured on the call at the lower layer (ISDN, ACC or L2TP). The default is CALL.

The CBDELAY parameter specifies the delay, in tenths of a second, between bringing down a call for callback and actually making the call back to the peer. This parameter is used to handle the different timing requirements of various ISDN switches and is only valid for PPP links over ISDN calls and when the callback mode is REQUEST. The default is 1.

The CBMODE parameter specifies whether a callback request will be made or accepted during the LCP negotiation. If REQUEST is specified a request will be made for callback. If ACCEPT is specified requests for callback received from the peer will be accepted and processed, however AUTHENTICATION must be set to PAP or CHAP. If OFF is specified no callback requests will be made and callback requests will not be accepted. The default is OFF.

The CBNUMBER parameter specifies the number to include when requesting a callback with the CBOPERATION parameter set to E164NUMBER. The number specified should be a phone number as specified in the E.164 standard.

The CBOPERATION parameter specifies the callback operation to be included in the callback request to specify to the peer how to determine the callback number. If USERAUTH is specified the peer will use the username and password supplied during authentication to look up the callback number. If

E164NUMBER is specified the callback number specified by the CBNUMBER parameter is included in the callback request. The default is USERAUTH.

The COMPALGORITHM parameter specifies the compression algorithm to use when compressing and decompressing PPP packets. If PREDICTOR is specified the Predictor algorithm will be used with type 1 encapsulation as specified in RFC 1978. If STACLZS is specified the Stac LZS algorithm will be used as specified in RFC 1974. The default is STACLZS.

The COMPRESSION parameter enables or disables the use of compression for the interface. When used with multilink, setting COMPRESSION to ON will compress the packets before they are sent to the individual links. Setting COMPRESSION to LINK will enable compression for the link specified by the OVER parameter. The default is OFF. The LINK option should only be used when compression is required on some physical interfaces and not on others. For example, if a PPP multilink uses a compressing modem link and a normal dedicated leased line, COMPRESSION should be set to OFF on the physical interface to which the modem is connected, and LINK for the physical interface to which the dedicated leased line is connected. If compression is required on all physical interfaces of a PPP interface, the COMPRESSION parameter should be set to ON.

The CONFIGURE parameter sets the number of configure requests sent before some action is taken. For the LCP the action is to reset the hardware and start again. For all other protocols the action is to give up. The default is CONTINUOUS, which means that requests will be sent continuously.

The DEBUGMAXBYTES parameter specifies the maximum number of bytes that are displayed for each packet when the PACKET debug option is enabled. The default is 32.

The DESCRIPTION parameter specifies a user-defined description for the interface, to make it easier to distinguish between a number of PPP interfaces.

The DNSPRIMARY parameter specifies the IP address to pass to a peer when it requests a primary DNS address using the IPCP primary DNS option.

The DNSSECONDARY parameter specifies the IP address to pass to a peer when it requests a secondary DNS address using the IPCP secondary DNS option.

The DOWNTIME parameter specifies the time, in seconds, that the PPP interface must have a total utilisation (as a percentage) below the threshold specified by the DOWNRATE parameter, before a channel is closed. The default is 60 for DOWNTIME and 20 for DOWNRATE. The UPRATE, UPTIME, DOWNRATE and DOWNTIME parameters are used in conjunction with the TYPE parameter to configure bandwidth on demand.

The ECHO parameter specifies whether or not LCP *Echo Request* and *Echo Reply* messages are used to determine link quality. If three consecutive *Echo Request* messages are transmitted without receiving an *Echo Reply* response, the link is deemed to be down. The ECHO and LQR parameters are mutually exclusive. If ECHO is enabled, LQR will be disabled. If LQR is enabled, ECHO will be set to OFF. If OFF is specified, *Echo Request* messages will not be transmitted. If ON is specified, *Echo Request* messages will be transmitted every 60 seconds. If a period in seconds is specified, *Echo Request* messages are transmitted at the specified interval.

The ENCRYPTION parameter enables or disables the use of encryption for the interface. The default is OFF.

For security reasons the ENCRYPTION parameter will only be accepted if the user has SECURITY OFFICER privilege.

The FRAGMENT parameter applies only to a multilink bundle interface, and determines whether packets are fragmented or not. The default is OFF. Fragmentation must be disabled if compression is required.

The FRAGOVERHEAD parameter specifies the maximum allowable overhead, as a percentage, for fragmenting packets using the variable fragmentation scheme for multilink PPP. If this limit will be exceeded for any packet the packet is fragmented using the fixed fragmentation scheme. The default is 5. The variable fragmentation scheme spreads the packet over all the links in the multilink bundle by splitting the packet into variable sized fragments to match the speed of individual links. Larger fragments are transmitted over faster links, thereby providing an inherent load balancing scheme. The fixed fragmentation scheme spreads the packet over all the links in the multilink bundle by splitting the packet into equal fixed sized fragments. If the number of links is large and the packet is relatively small a fragment is not transmitted over every link.

The IDLE parameter controls the dial-on-demand feature. If ON is specified, dial-on-demand is enabled with a default timer of 60 seconds. If a time is specified, dial-on-demand is enabled with the timer set to the specified time. If OFF is specified, dial-on-demand is disabled. When the dial-on-demand feature is activated, PPP brings up the link when there is traffic to be sent, and takes down the link when there has been no traffic for the specified timer period. The effect on a PPP interface using an ISDN call will be to connect the call when traffic is to be sent and disconnect the call when no traffic has been sent or received for the specified timer period. For other physical interfaces, this parameter has no effect, as the links are always connected. The default is OFF.

The IPREQUEST parameter specifies whether or not a request will be made for an IP address to be allocated by the peer during the IPCP negotiation. If ON is specified a request will be made. If OFF is specified a request will not be specified. The default is OFF.

The LQR parameter sets the LQR timer. If ON is specified, LQR is enabled with a default timer of 60 seconds. If a time is specified, LQR is enabled with the timer set to the specified time. If OFF is specified, LQR is disabled. The default is ON.

The MAGIC parameter enables or disables negotiation of the magic number option. The default is ON. The magic number is used to determine if a interface is looped back. The interface will not reach the OPENED state if there is a loopback.

The MODEM parameter specifies the state of synchronous modem control. The default is OFF. If ON is specified, the router will manipulate the DTR signal to trigger the modem to make a call whenever there is traffic (IDLE=ON) or when a backup link is required (TYPE=SECONDARY). Raising DTR to the modem triggers the modem to initiate a call to the modem at the other end of the link and enter data transfer mode. The router will keep the DTR signal to the modem raised, and will respond to the modem raising the DSR signal by acti-

vating the PPP interface. This parameter is only valid when the OVER parameter specifies a synchronous interface.

The NUMBER parameter specifies the number of physical interfaces to be created. This parameter is only valid when the OVER parameter specifies an ISDN call as the physical interface. The default is 1.

The NULLFRAGTIMER parameter specifies the maximum time, in seconds, a link in a multilink bundle may be idle before a NULL fragment is transmitted over the link. NULL fragments are used to keep the last sequence number transmitted over the link up to date. The default is 3.

The PASSWORD parameter specifies the password to use when the peer requests authentication using either CHAP or PAP. This is normally required for network lines between routers, for which an authentication protocol has been selected with the AUTHENTICATION parameter.

The PREDCHECK parameter specifies the type of CRC to be used for Predictor compression. The Predictor RFC specifies using CRC-16, however some router manufacturers have implemented Predictor with CRC-CCITT which is the CRC specified in RFC 1662, “PPP in HDLC-link Framing”. This value is not negotiated so the same value needs to be configured at both ends of the link for Predictor compression to work correctly.

The RESTART parameter specifies the time between successive retransmissions of unacknowledged configure requests or terminate requests. The default is 3 seconds.

The STACCHECK parameter specifies the check mode to used for the Stac LZS compression algorithm. If SEQUENCE is specified an incrementing sequence number is used to determine whether a packet has been lost and therefore whether the compression history needs to be reset. If LCB is specified an LCB value is used to determine if an error has occurred in a packet. The default is SEQUENCE.

The STARENTITY parameter specifies the star entity and the encryption algorithm to be used by the encryption channel configured by the PPP interface. This parameter must be specified if PPP encryption is enabled.

The TERMINATE parameter sets the number of terminate requests sent when trying to close a link before it is assumed the link is down. The default is 2. The CONTINUOUS option specifies that requests will be sent continuously.

The TYPE parameter specifies the role of the physical interface for bandwidth on demand and leased line backup. The default is PRIMARY. If PRIMARY is specified, the link will be kept open all the time (IDLE=OFF) or opened whenever there is traffic (IDLE=ON). If SECONDARY is specified, the link will be opened only when the associated primary link fails. If DEMAND is specified, the link will be opened only when the additional bandwidth is required.

To configure bandwidth on demand the ISDN channels are given a TYPE of DEMAND when they are added to the PPP interface. Adding one channel with a type of PRIMARY and other channels with a TYPE of DEMAND will ensure that there is always one channel available. If all channels are assigned a TYPE of DEMAND then there will be no channels open when there is no traffic, some traffic will cause one channel to be opened and continuous traffic will cause other channels to be opened. If there is one channel remaining opened then the IDLE timer is used to determine when this channel should be closed. In this case it is recommended that the IDLE timer not be set to OFF.

To configure leased line backup the synchronous link is assigned a TYPE of PRIMARY and the ISDN call is assigned a TYPE of SECONDARY. When the primary link fails, LQR detects the failure and resets the link causing configure requests to be transmitted. If the primary link fails to reach the OPENED state after a number of configure request packets have been transmitted, the secondary link is activated. The number of configure request packets transmitted and the interval between successive retransmissions of configure request packets is controlled by the CONFIGURE and RESTART parameters. The CONFIGURE parameter needs to be specified as the default is CONTINUOUS. The time interval between link failure and activation of the secondary link depends on the LQR timer, and the CONFIGURE and RESTART parameters.

The UPTIME parameter specifies the time, in seconds, that the PPP interface must have a total utilisation (as a percentage) above the threshold specified by the UPRATE parameter, before an additional channel is opened. The default is 30 for UPTIME and 80 for UPRATE. The UPRATE, UPTIME, DOWNRATE and DOWNTIME parameters are used in conjunction with the TYPE parameter to configure bandwidth on demand.

The USERNAME parameter specifies the username to be used when generating PAP authentication requests and when responding to CHAP authentication challenges. If the USERNAME is not set the router's system name will be used by default.

The WINSPRIMARY parameter specifies the IP address to pass to a peer when it requests a primary WINS server address using the IPCP primary WINS server option.

The WINSSECONDARY parameter specifies the IP address to pass to a peer when it requests a primary WINS server address using the IPCP secondary WINS server option.

Examples

To disable compression on the synchronous interface 0 link of PPP interface 1, use the command:

```
SET PPP=1 OVER=SYN0 COMP=OFF
```

See Also

ADD PPP
CREATE PPP
SHOW PPP

SET PPP TEMPLATE

Syntax

```
SET PPP TEMPLATE=template [AUTHENTICATION={CHAP|EITHER|
   PAP|NONE}] [BAP={ON|OFF}] [BAPMODE={CALL|CALLBACK}]
   [CBDELAY=1..100] [CBMODE={ACCEPT|OFF|REQUEST}]
   [CBNUMBER=e164number] [CBOPERATION={E164NUMBER|
   USERAUTH}] [COMPALGORITHM={PREDICTOR|STACLZS}]
   [COMPRESSION={ON|OFF|LINK}] [DEBUGMAXBYTES=16..256]
   [DESCRIPTION=description] [ECHO={ON|OFF|period}]
   [ENCRYPTION={ON|OFF}] [FRAGMENT={ON|OFF}]
   [FRAGOVERHEAD=0..100] [IDLE={ON|OFF|time}]
   [IPREQUEST={ON|OFF}] [LOGIN={ALL|RADIUS|TACACS|USER}]
   [LQR={ON|OFF|time}] [MAGIC={ON|OFF}] [MAXLINKS=1..64]
   [NULLFRAGTIMER=time] [PASSWORD=password]
   [PREDCHECK={CRC16|CRCCCITT}] [RESTART=time]
   [STACCHECK={LCB|SEQUENCE}] [STARENTITY=1..255]
   [USERNAME=username]
```

where:

- *template* is a number in the range 0 to 31.
- *e164number* is the phone number to dial when performing callback. It may contain digits (0–9) and should be a valid phone number as described in CCITT standard E.164.
- *description* is a character string, 1 to 70 characters in length. Valid characters are any printable character.
- *period* is a decimal number in the range 1 to 4294967295.
- *time* is a timer value in seconds.
- *password* is the password to use for authentication, 1 to 32 characters in length. It may contain any printable character, and is case sensitive.
- *username* is the username to use for authentication, 1 to 32 characters in length. It may contain any printable character, and is case sensitive.

Description

This command modifies an existing PPP template that is used to configure dynamic PPP interfaces that are created when an ISDN, ACC or L2TP call is activated.

The TEMPLATE parameter specifies the number of the template to modify. The specified template must already exist.

The AUTHENTICATION parameter specifies the authentication protocol to be used on the physical interface or channel. If CHAP is specified, the Challenge-Handshake Authentication Protocol (CHAP) is used. If PAP is specified, the Password Authentication Protocol (PAP) is used. If EITHER is specified, the router uses the option negotiation process to negotiate the authentication protocol to be used with the device at the remote end of the link, specifying CHAP as the first choice. If NONE is specified, no authentication protocol is used. The default is NONE.

The BAP parameter specifies whether or not the Bandwidth Allocation Protocol will be used for negotiating the activation of demand PPP links. The default is ON.

The BAPMODE parameter specifies which peer originates another link to add to the multilink bundle. For CALLBACK mode, the number to call must be

configured on the call at the lower layer (ISDN, ACC or L2TP). The default is CALL.

The CBDELAY parameter specifies the delay, in tenths of a second, between bringing down a call for callback and actually making the call back to the peer. This parameter is used to handle the different timing requirements of various ISDN switches and is only valid for PPP links over ISDN calls and when the callback mode is REQUEST. The default is 1.

The CBMODE parameter specifies whether a callback request will be made or accepted during the LCP negotiation. If REQUEST is specified a request will be made for callback. If ACCEPT is specified requests for callback received from the peer will be accepted and processed, however AUTHENTICATION must be set to PAP or CHAP. If OFF is specified no callback requests will be made and callback requests will not be accepted. The default is OFF.

The CBNUMBER parameter specifies the number to include when requesting a callback with the CBOPERATION parameter set to E164NUMBER. The number specified should be a phone number as specified in the E.164 standard.

The CBOPERATION parameter specifies the callback operation to be included in the callback request to specify to the peer how to determine the callback number. If USERAUTH is specified the peer will use the username and password supplied during authentication to look up the callback number. If E164NUMBER is specified the callback number specified by the CBNUMBER parameter is included in the callback request. The default is USERAUTH.

The COMPALGORITHM parameter specifies the compression algorithm to use when compressing and decompressing PPP packets. If PREDICTOR is specified the Predictor algorithm will be used with type 1 encapsulation as specified in RFC 1978. If STACLZS is specified the Stac LZS algorithm will be used as specified in RFC 1974. The default is STACLZS.

The COMPRESSION parameter enables or disables the use of compression for the interface. When used with multilink, setting COMPRESSION to ON will compress the packets before they are sent to the individual links. Setting COMPRESSION to LINK will enable compression for the link specified by the OVER parameter. The default is OFF. The LINK option should only be used when compression is required on some physical interfaces and not on others. For example, if a PPP multilink uses a compressing modem link and a normal dedicated leased line, COMPRESSION should be set to OFF on the physical interface to which the modem is connected, and LINK for the physical interface to which the dedicated leased line is connected. If compression is required on all physical interfaces of a PPP interface, the COMPRESSION parameter should be set to ON.

The DEBUGMAXBYTES parameter specifies the maximum number of bytes that are displayed for each packet when the PACKET debug option is enabled. The default is 32.

The DESCRIPTION parameter specifies a user-defined description for the interface, to make it easier to distinguish between a number of PPP interfaces.

The ECHO parameter specifies whether or not LCP *Echo Request* and *Echo Reply* messages are used to determine link quality. If three consecutive *Echo Request* messages are transmitted without receiving an *Echo Reply* response, the link is deemed to be down. The ECHO and LQR parameters are mutually exclusive. If ECHO is enabled, LQR will be disabled. If LQR is enabled, ECHO will be set to OFF. If OFF is specified, *Echo Request* messages will not be trans-

mitted. If ON is specified, *Echo Request* messages will be transmitted every 60 seconds. If a period in seconds is specified, *Echo Request* messages are transmitted at the specified interval.

The ENCRYPTION parameter enables or disables the use of encryption for the interface. The default is OFF.

For security reasons the ENCRYPTION parameter will only be accepted if the user has SECURITY OFFICER privilege.

The FRAGMENT parameter applies only to a multilink bundle interface, and determines whether packets are fragmented or not. The default is OFF. Fragmentation must be disabled if compression is required.

The FRAGOVERHEAD parameter specifies the maximum allowable overhead, as a percentage, for fragmenting packets using the variable fragmentation scheme for multilink PPP. If this limit will be exceeded for any packet the packet is fragmented using the fixed fragmentation scheme. The default is 5. The variable fragmentation scheme spreads the packet over all the links in the multilink bundle by splitting the packet into variable sized fragments to match the speed of individual links. Larger fragments are transmitted over faster links, thereby providing an inherent load balancing scheme. The fixed fragmentation scheme spreads the packet over all the links in the multilink bundle by splitting the packet into equal fixed sized fragments. If the number of links is large and the packet is relatively small a fragment is not transmitted over every link.

The IDLE parameter controls the dial-on-demand feature. If ON is specified, dial-on-demand is enabled with a default timer of 60 seconds. If a time is specified, dial-on-demand is enabled with the timer set to the specified time. If OFF is specified, dial-on-demand is disabled. When the dial-on-demand feature is activated, PPP brings up the link when there is traffic to be sent, and takes down the link when there has been no traffic for the specified timer period. The effect on a PPP interface using an ISDN call will be to connect the call when traffic is to be sent and disconnect the call when no traffic has been sent or received for the specified timer period. For other physical interfaces, this parameter has no effect, as the links are always connected. The default is OFF.

The IPREQUEST parameter specifies whether or not a request will be made for an IP address to be allocated by the peer during the IPCP negotiation. If ON is specified a request will be made. If OFF is specified a request will not be specified. The default is OFF.

The LOGIN parameter specifies which login procedure the call creating this dynamic interface must use when it is activated. If RADIUS is specified, the router will send requests to the configured RADIUS server(s) to authenticate the call. If TACACS is specified, the router will send requests to the configured TACACS server(s) to authenticate the call. If USER is specified, the router will check the User Authentication Database to authenticate the call. If ALL is specified, the router will try all methods to authenticate the call.

The LQR parameter sets the LQR timer. If ON is specified, LQR is enabled with a default timer of 60 seconds. If a time is specified, LQR is enabled with the timer set to the specified time. If OFF is specified, LQR is disabled. The default is ON.

The MAGIC parameter enables or disables negotiation of the magic number option. The default is ON. The magic number is used to determine if a interface is looped back. The interface will not reach the OPENED state if there is a loop-back.

The MAXLINKS parameter specifies the maximum number of links allowed in a multilink PPP interface created using this template.

The NULLFRAGTIMER parameter specifies the maximum time, in seconds, a link in a multilink bundle may be idle before a NULL fragment is transmitted over the link. NULL fragments are used to keep the last sequence number transmitted over the link up to date. The default is 3.

The PASSWORD parameter specifies the password to use when the peer requests authentication using either CHAP or PAP. This is normally required for network lines between routers, for which an authentication protocol has been selected with the AUTHENTICATION parameter.

The PREDCHECK parameter specifies the type of CRC to be used for Predictor compression. The Predictor RFC specifies using CRC-16, however some router manufacturers have implemented Predictor with CRC-CCITT which is the CRC specified in RFC 1662, “PPP in HDLC-link Framing”. This value is not negotiated so the same value needs to be configured at both ends of the link for Predictor compression to work correctly.

The RESTART parameter specifies the time between successive retransmissions of unacknowledged configure requests or terminate requests. The default is 3 seconds.

The STACCHECK parameter specifies the check mode to used for the Stac LZS compression algorithm. If SEQUENCE is specified an incrementing sequence number is used to determine whether a packet has been lost and therefore whether the compression history needs to be reset. If LCB is specified an LCB value is used to determine if an error has occurred in a packet. The default is SEQUENCE.

The STARENTITY parameter specifies the star entity and the encryption algorithm to be used by the encryption channel configured by the PPP interface. This parameter must be specified if PPP encryption is enabled.

The USERNAME parameter specifies the username to be used when generating PAP authentication requests and when responding to CHAP authentication challenges. If the USERNAME is not set the router’s system name will be used by default.

Examples

To modify template 1 to use LCP Echo for link quality management, use the command:

```
CREATE PPP TEMPLATE=1 ECHO=ON
```

See Also

CREATE PPP TEMPLATE
DESTROY PPP TEMPLATE
DISABLE PPP TEMPLATE DEBUG
ENABLE PPP TEMPLATE DEBUG
SHOW PPP TEMPLATE

SHOW PPP

Syntax `SHOW PPP[=`*`ppp-interface`*`]`

where:

- *ppp-interface* is the PPP interface number.

Description This command displays a list of each PPP interface, users of the interface, physical interfaces that the interface is running over and the current state of the interface (Figure 3-14 on page 3-65, Table 3-7 on page 3-65).

Figure 3-14: Example output from the SHOW PPP command.

```
Name            Enabled  ifIndex  Over                 CP          State
-------------------------------------------------------------------------
ppp0              YES      04                          IPCP        OPENED
                                    syn0                LCP         OPENED
                                    isdn-demand         LCP         OPENED
-------------------------------------------------------------------------
```

Table 3-7: Parameters displayed in the output of the SHOW PPP command.

Parameter	Meaning
Name	The name of the PPP interface.
Enabled	YES if the PPP interface is enabled; NO if it is disabled.
IfIndex	The value of ifIndex for the PPP interface.
Over	The physical layer(s) used by the PPP interface; one of SYN*n*, ISDN-*callname*, ACC-*callname*, MIOX*n-circuitname*, TNL-*callname* or TDM-*groupname*.
CP	A list of the network and link control protocols running over the PPP interface; one or more of "IPCP", "IPXCP", "BCP", "DNCP", "ATCP", "LCP", "CCP", "ILCCP", "ECP", "BACP" or "MULTI".
State	The state of the PPP links; one of "INITIAL", "STARTING", "CLOSED", "STOPPED", "CLOSING", "STOPPING", "REQ SENT", "ACK RCVD", "ACK SENT" or "OPENED".

Examples To display information about PPP interface 2, use the command:

```
SHOW PPP=2
```

See Also SHOW PPP CONFIG
SHOW PPP COUNT

SHOW PPP CONFIG

Syntax `SHOW PPP[=`*`ppp-interface`*`] CONFIG`

where:

- *ppp-interface* is the PPP interface number.

Description This command displays the configuration of a PPP interface (Figure 3-15 on page 3-66, Table 3-8 on page 3-67).

Figure 3-15: Example output from the SHOW PPP CONFIG command.

```
Interface - description
  Parameter                        Configured                Negotiated
-------------------------------------------------------------------------------
ppp0 - Link to Southern Regional Office
                                                        Local            Peer
  Bandwidth Allocation Protocol           ON
  Bandwidth Allocation Call Mode        CALL
  Multilink Fragmentation                OFF
  Acceptable Fragment Overhead (%)         5
  Null Fragment Timer (seconds)            3
  Idle Timer (seconds)                    60
  Maximum Receive Unit (bytes)          1656            NONE            NONE
  Compression                             ON              ON              ON
  Encryption                             OFF             OFF             OFF
  Username                           NOT SET
  Password                           NOT SET
  Bundle Endpoint Discr Class              0
  Bundle Endpoint Discr Value             []
  Bundle Username                    NOT SET
acc-btb
  Type                               primary
  Restart Timer (seconds)                  3
  Max-Configure                    continuous
  Max-Terminate                            2
  Echo Request Timer (seconds)           OFF
  Callback Mode                          OFF
  Link Compression                        ON              ON              ON
  LQR Timer (seconds)                     60             OFF             OFF
  Magic Number                            ON             OFF             OFF
  Link Discriminator                    0000             OFF             OFF
  Link Endpoint Discr Class                0
  Link Endpoint Discr Value
  Authentication                         PAP            NONE            NONE
  Authentication Mode                  INOUT
  Utilisation (%)                          0
Compression
  Algorithm                          STACLZS         STACLZS         STACLZS
  Stac LZS Checkmode                SEQUENCE        SEQUENCE        SEQUENCE
IP
  IP Compression Protocol                NONE            NONE            NONE
  IP Address Request                     OFF
  IP Address                     192.168.1.1     192.168.1.1     192.168.1.2
  Primary DNS Address            192.168.2.3            NONE            NONE
  Secondary DNS Address          192.168.5.1                            NONE
  Primary WinS Address           192.168.5.5                            NONE
  Secondary WinS Address             NOT SET                            NONE
Debug
  Maximum packet bytes to display         22
-------------------------------------------------------------------------------
```

Table 3-8: Parameters displayed in the output of the SHOW PPP CONFIG command.

Parameter	Meaning
Configured	This column specifies the value that has been configured for a parameter. The value may be modified by the negotiation process between the local and remote ends of the PPP link.
Negotiated/Local	For a link that is in the OPENED state, this column specifies the value that the local end of the link will use for a parameter, as a result of the negotiation process. For a link that is not in the OPENED state, this column displays the initial value for a parameter.
Negotiated/Peer	For a link that is in the OPENED state, this column specifies the value that the remote end of the link will use for a parameter, as a result of the negotiation process. For a link that is not in the OPENED state, this column displays the initial value for a parameter.
ppp<*n*> - <*description*>	The name and description of the interface. Following fields display information about the interface as a whole.
Bandwidth Allocation Protocol	Whether or not the Bandwidth Allocation Protocol is enabled on the interface; one of "ON" or "OFF".
Bandwidth Allocation Call Mode	The call mode for the Bandwidth Allocation Protocol, if the Bandwidth Allocation Protocol is enabled on the interface; one of "CALL" or "CALLBACK".
Multilink fragmentation	Whether or not multilink packets may be fragmented; one of "ON" or "OFF".
Acceptable Fragment Overhead (%)	The maximum amount of overhead allowed to be added to each packet due to variable fragmentation. If this level is exceeded when fragmentation of a packet is done using the variable fragmentation scheme, then the fixed fragmentation scheme is used instead.
Null Fragment Timer (seconds)	The time, in seconds, that the link must be idle for before a Null fragment is sent on a link in a multilink bundle.
Idle Timer (seconds)	The length of time, in seconds, a link must be idle before it is disconnected, or "OFF" if the idle timer is disabled.
Maximum Receive Unit (bytes)	The maximum allowable length for packets received at the PPP layer. The MRU of the peer is used as the MTU of the upper layers so that they don't transmit anything that is too long for the peer to handle.
Compression	Whether or not compression is enabled for the entire PPP interface; one of "ON" or "OFF".
Encryption	Whether or not encryption is enabled for the entire PPP interface; one of "ON" or "OFF".
Username	The username used by the PPP interface for both PAP and CHAP authentication, or "NOT SET" if a username has not been set.
Password	Whether or not a password has been set for the entire PPP interface; one of "SET" or "NOT SET".
Up Rate (%utilisation)	The utilisation level on the link at which an additional channel is opened, if the interface has on-demand links.
Up Time (seconds)	The time, in seconds, that the utilisation level on the link must exceed *Up Rate* before an additional channel is opened, if the interface has on-demand links.

Table 3-8: Parameters displayed in the output of the SHOW PPP CONFIG command. (Continued)

Parameter	Meaning
Down Rate (%utilisation)	The utilisation level on the link below which a channel is closed, if the interface has on-demand links.
Down Time (seconds)	The time, in seconds, that the utilisation level on the link must be below *Down Rate* before a channel is closed, if the interface has on-demand links.
Bundle Endpoint Discr Class	The class of endpoint discriminator used to uniquely identify this link's endpoint.
Bundle Endpoint Discr Value	The value, in hexadecimal, of the endpoint discriminator used to uniquely identify this link's endpoint.
Bundle Username	The username assigned to the multilink bundle, or "NOT SET" if a username has not been set.
LCP Information	**This section is repeated once for each LCP (physical interface) operating over the PPP interface.**
<lcp-name>	The name of an LCP operating over this PPP interface. Following fields display information about this LCP (link).
Number of primary channels	The number of channels with a TYPE of PRIMARY carried over the ISDN call, if this physical interface is an ISDN call.
Number of secondary channels	The number of channels with a TYPE of SECONDARY carried over the ISDN call, if this physical interface is an ISDN call.
Number of demand channels	The number of channels with a TYPE of DEMAND carried over the ISDN call, if this physical interface is an ISDN call.
Type	The role of this physical interface for bandwidth on demand and leased line backup; one of "demand", "primary" or "secondary".
Modem Control	Whether or not modem control is enabled (only valid on synchronous interfaces); one of "ON" or "OFF".
Restart Timer	The time, in seconds, between configure requests for this physical interface.
Max-Configure	The maximum number of configure requests sent before PPP gives up trying to open this link, or "continuous".
Max-Terminate	The maximum number of Terminate requests sent before PPP gives up trying to open this link and declares this link down, or "continuous".
Echo Request Timer (seconds)	The time, in seconds, between transmissions of LCP *Echo Request* messages when LCP *Echo Request*/*Echo Reply* messages are used to monitor link state, or "OFF" if LQR is used to determine link status.
Callback Mode	Whether this link will request callback, accept callback or do neither; one of "REQUEST", "ACCEPT" or "OFF".
Callback Operation	The callback operation to include in the callback request when the callback mode is REQUEST; one of "USERAUTH" or "E164NUMBER". This field is only displayed if *Callback Mode* is set to "REQUEST".

Table 3-8: Parameters displayed in the output of the SHOW PPP CONFIG command. (Continued)

Parameter	Meaning
Callback Number	The callback number included in callback requests when the callback mode is REQUEST and the callback operation is E164NUMBER. This field is only displayed if *Callback Mode* is set to "REQUEST" and *Callback Operation* is set to "E164NUMBER".
Callback Delay (tenths of a second)	The delay, in tenths of a second, between deactivating a call for callback and making the return call. This field is only displayed if *Callback Mode* is set to "ACCEPT".
Link Compression	Whether or not compression is enabled for this link rather than the entire PPP interface; one of "ON" or "OFF".
LQR Timer (seconds)	The time in seconds between LQR packets transmitted over this physical interface.
Magic Number	Whether or not the magic number option is enabled for this physical interface; one of "ON" or "OFF".
Link Discriminator	The link discriminator value for this physical interface, or "OFF" if the link discriminator LCP option is not enabled.
Link Endpoint Discr Class	The class of link endpoint discriminator assigned to this end of the physical interface.
Link Endpoint Discr Value	The value the of link endpoint discriminator assigned to this end of the physical interface, expressed in hexadecimal.
Authentication	The authentication protocol in use on this physical interface; one of "NONE", "PAP", "CHAP" or "EITHER".
Authentication Mode	Whether authentication will be requested on incoming ISDN calls, outgoing ISDN calls, or both incoming and outgoing ISDN calls; one of "IN", "OUT" or "INOUT".
Utilisation (%)	The bandwidth utilisation, as a percentage of time the interface is transmitting data, for this physical interface.
Link Compression	Information about link compression on this physical interface if link compression is enabled on this physical interface.
Algorithm	The compression algorithm to use for compressing packets on this physical interface; one of "PREDICTOR" or "STAC_LZS".
Stac LZS Checkmode	The check mode used by the Stac LZS compression algorithm to determine if a decompression history is unsynchronised on this physical interface; one of "NONE", "LCB", "CRC", "SEQUENCE" or "EXTENDED".
Predictor LZS Checkmode	The check mode used by the Predictor compression algorithm to determine if a decompression history is unsynchronised on this physical interface; one of "CRC-16" or "CRC-CCITT".
Channel Information	**This section is displayed only if the LCP (physical interface) is an ISDN interface, and is repeated once for each channel in the physical interface. Basic Rate ISDN interfaces have 2 channels. Primary Rate ISDN interfaces has 30 channels.**
bri<*n*> - channel <*n*> pri<*n*> - channel <*n*>	The interface and channel number of physical interfaces that are ISDN calls. Following fields display information specific to this channel.

Table 3-8: Parameters displayed in the output of the SHOW PPP CONFIG command. (Continued)

Parameter	Meaning
Type	The role of this channel for bandwidth on demand and leased line backup; one of "demand", "primary" or "secondary".
Utilisation (%)	The bandwidth utilisation, as a percentage of time the interface is transmitting data, for the physical interface.
Link Compression	Whether or not compression is enabled for the link rather than the entire PPP interface; one of "ON" or "OFF".
LQR Timer (seconds)	The time in seconds between LQR packets transmitted over the physical interface.
Magic Number	Whether or not the magic number option is enabled for the physical interface; one of "ON" or "OFF".
Link Discriminator	The link discriminator value for the physical interface, or "OFF" if the link discriminator LCP option is not enabled.
Link Endpoint Discr Class	The class of link endpoint discriminator assigned to this end of the physical interface.
Link Endpoint Discr Value	The value the of link endpoint discriminator assigned to this end of the physical interface, expressed in hexadecimal.
Authentication	The authentication protocol in use on the physical interface; one of "NONE", "PAP", "CHAP" or "EITHER".
NCP Information	**This section is repeated once for each NCP configured on the PPP interface.**
Encryption	Information about encryption on the PPP interface, if encryption is enabled on the interface.
Star Entity Identifier	The star entity and encryption algorithm used on the PPP interface.
Link Compression	Information about link compression on the PPP interface if link compression is enabled on the PPP interface.
Algorithm	The compression algorithm to use for compressing packets on the PPP interface; one of "PREDICTOR" or "STAC_LZS".
Stac LZS Checkmode	The check mode used by the Stac LZS compression algorithm to determine if a decompression history is unsynchronised on the PPP interface; one of "NONE", "LCB", "CRC", "SEQUENCE" or "EXTENDED".
Predictor LZS Checkmode	The check mode used by the Predictor compression algorithm to determine if a decompression history is unsynchronised on the PPP interface; one of "CRC-16" or "CRC-CCITT".
IP	Information about the IP NCP on the PPP interface, if IP is enabled on this PPP interface.
IP Compression Protocol	The IP compression protocol enabled on the PPP interface; one of "VJC" (Van Jacobson header compression) or "NONE".
IP Address Request	Whether or not an IP address will be requested from the peer during IPCP negotiation; one of "ON" or "OFF".
IP Address	The IP address configured at each end of the link, "0.0.0.0" if the PPP interface is an unnumbered interface, or "NONE" if an IP address has not been assigned.

Table 3-8: Parameters displayed in the output of the SHOW PPP CONFIG command. (Continued)

Parameter	Meaning
Primary DNS Address	The IP address of the primary DNS server, passed to a peer in response to an IPCP primary DNS request.
Secondary DNS Address	The IP address of the secondary DNS server, passed to a peer in response to an IPCP secondary DNS request.
Primary WinS Address	The IP address of the primary WINS server, passed to a peer in response to an IPCP primary WINS server request.
Secondary WinS Address	The IP address of the secondary WINS server, passed to a peer in response to an IPCP secondary WINS server request.
Debug	Information about debugging on the PPP interface.
Maximum packet bytes to display	The maximum number of bytes of each PPP packet displayed by the PACKET debugging option.

Examples To display the configuration for PPP interface 2, use the command:

```
SHOW PPP=2 CONFIG
```

See Also SHOW PPP
SHOW PPP COUNT

SHOW PPP COUNT

Syntax `SHOW PPP[=`*`ppp-interface`*`] COUNT[={INTERFACE|LCP|MULTILINK|NCP}]`

where:

- *ppp-interface* is the PPP interface number.

Description This command displays the interface MIB entry and counters for users of the interface. If INTERFACE is specified, counters from the Interfaces table of the MIB are displayed (Figure 3-16 on page 3-71, Table 3-9 on page 3-72). If LCP is specified, counters for the LCP, LQR, CCP, ECP and any authentication protocols are displayed (Figure 3-17 on page 3-73, Table 3-10 on page 3-74). If MULTILINK is specified, counters for the multilink protocol are displayed (Figure 3-18 on page 3-79, Table 3-11 on page 3-79). If NCP is specified, counters for the NCPs are displayed (Figure 3-19 on page 3-80, Table 3-12 on page 3-80). If a category is not specified all counters are displayed, including those for BAP and BACP (Table 3-13 on page 3-81).

Figure 3-16: Example output from the SHOW PPP COUNT=INTERFACE command.

```
ppp0                 1519 seconds     Last change at:        974 seconds
Interface Counters
  ifInOctets               116554     ifOutOctets                 91792
  ifInUcastPkts                 0     ifOutUcastPkts                  0
  ifInNUcastPkts             2098     ifOutNUcastPkts              1538
  ifInDiscards                  0     ifOutDiscards                   0
  ifInErrors                    3     ifOutErrors                     0
  ifInUnknownProtos             0     ifOutQLen                       0
```

Table 3-9: Parameters displayed in the output of the SHOW PPP COUNT=INTERFACE command.

Parameter	Meaning
ppp0	The interface name.
seconds	The time (in seconds) since the interface was last re-initialised.
Last change at	The time (in seconds) since the interface entered its current operational state.
ifInOctets	The total number of octets received over the interface, including two octets per frame for PPP address and control information, two octets per frame for the FCS, one octet per frame for a flag and two octets per frame for the PPP header (six for multilink), and the number of octets in the user data packets and PPP control packets.
ifInUcastPkts	The total number of subnetwork-unicast packets delivered to a higher-layer protocol.
ifInNUcastPkts	The total number of non-unicast packets delivered to a higher-layer protocol.
ifInDiscards	The total number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
ifInErrors	The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
ifInUnknownProtos	The total number of packets received via the interface which were discarded because of an unknown or unsupported protocol.
ifOutOctets	The total number of octets transmitted over the interface, including two octets per frame for PPP address and control information, two octets per frame for the FCS, one octet per frame for a flag and two octets per frame for the PPP header (six for multilink), and the number of octets in the user data packets and PPP control packets.
ifOutUcastPkts	The total number of packets that higher-layer protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
ifOutNUcastPkts	The total number of packets that higher-layer protocols requested be transmitted to a non-unicast address, including those that were discarded or not sent.
ifOutDiscards	The total number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
ifOutErrors	The total number of outbound packets that contained errors preventing them from being transmitted.
ifOutQLen	The length of the output packet queue.

Figure 3-17: Example output from the SHOW PPP COUNT=LCP command.

```
CCP
  inOctets                    52456     outOctets                   38959
  inUserPkts                   2101     outUserPkts                  1538
  inConfigureRequest              3     outConfigureRequest             3
  inConfigureAcknowledge          3     outConfigureAcknowledge         3
  inConfigureNAK                  0     outConfigureNAK                 0
  inConfigureReject               0     outConfigureReject              0
  inTerminateRequest              0     outTerminateRequest             0
  inTerminateAcknowledge          0     outTerminateAcknowledge         0
  inCodeReject                    0     outCodeReject                   0
  decodeSsuccesses             2098     encodeSuccesses              1538
  decodeFailures                  3     encodeFailures                  0
  decodeDiscards                  0     encodeDiscards                  0
  inResetRequests                 8     outResetRequests                3
  inResetAcks                     3     outResetAcks                    2
  encoEventsWithLcpDown           0

LQM    OVER: syn1
  lqrFailures                     0     loopbacksDetected               0

  inLQRs                         16     outLQRs                        16
  inPktLost                       0     outPktLost                      0
  inOctetLost                     0     outOctetLost                    0
                                        outLQRsLost                     0
                                        outLQRsTransit                  0

PAP    OVER: syn1
  inRequest                       1     outRequest                      0
  inAck                           0     outAck                          1
  inNak                           0     outNak                          0

LCP    OVER: syn1
  inOctets                    25316     outOctets                   19158
  inUserPkts                    929     outUserPkts                   749
  inConfigureRequest              3     outConfigureRequest             7
  inConfigureAcknowledge          3     outConfigureAcknowledge         3
  inConfigureNAK                  0     outConfigureNAK                 0
  inConfigureReject               3     outConfigureReject              0
  inTerminateRequest              0     outTerminateRequest             1
  inTerminateAcknowledge          1     outTerminateAcknowledge         0
  inCodeReject                    0     outCodeReject                   0
  inProtocolReject                3     outProtocolReject               0
  inEchoRequest                   0     outEchoRequest                  0
  inEchoReply                     0     outEchoReply                    0
  inDiscardRequest                0     outDiscardRequest               0
  echoFailures                    0     badEchoReplies                  0
```

Table 3-10: Parameters displayed in the output of the SHOW PPP COUNT=LCP command.

Parameter	Meaning
ECP	Information about the encryption control protocol (ECP).
inOctets	The number of octets received by the encryption protocol. This includes two octets per frame for the PPP encryption header, the number of octets of encrypted data received, and the number of octets in control protocol packets (ECP). For multilinks an extra six octets per frame are included for the multilink header.
inUserPkts	The number of packets received for the encryption control protocol.
inConfigureRequest	The number of *Configure-Request* packets received for the encryption control protocol.
inConfigureAcknowledge	The number of *Configure-Acknowledge* packets received for the encryption control protocol.
inConfigureNAK	The number of *Configure-NAK* packets received for the encryption control protocol.
inConfigureReject	The number of *Configure-Reject* packets received for encryption control protocol.
inTerminateRequest	The number of *Terminate-Request* packets received for encryption control protocol.
inTerminateAcknowledge	The number of *Terminate-Acknowledge* packets received for the encryption control protocol.
inCodeReject	The number of *Code-Reject* packets received for the encryption control protocol.
inResetRequests	The number of *Reset-Request* packets received to reset the encryption history.
inResetACKs	The number of *Reset-Acknowledge* packets received to reset the encryption history.
decodeSuccesses	The number of encrypted packets successfully decoded.
decodeFailures	The number of encrypted packets that failed to be decoded.
decodeDiscards	The number of packets to be decoded that were discarded.
getSessKeySuccesses	The number of times a session key has been retrieved from the STAR module.
getMktSuccesses	The number of times a master key table has been retrieved from the STAR module.
starEventsNotAttached	The number of times the PPP interface received an event from the STAR module when it was not attached.
abortedNegotiations	The number of times an ECP negotiation was aborted
outOctets	The number of octets transmitted by the encryption protocol. This includes two octets per frame for the PPP encryption header, the number of octets of encrypted data transmitted, and the number of octets in control protocol packets (ECP). For multilinks an extra six octets per frame are included for the multilink header.
outUserPkts	The number of packets transmitted by the encryption control protocol.
outConfigureRequest	The number of *Configure-Request* packets transmitted by the encryption control protocol.

Table 3-10: Parameters displayed in the output of the SHOW PPP COUNT=LCP command. (Continued)

Parameter	Meaning
outConfigureAcknowledge	The number of *Configure-Acknowledge* packets transmitted by the encryption control protocol.
outConfigureNAK	The number of *Configure-NAK* packets transmitted by the encryption control protocol.
outConfigureReject	The number of *Configure-Reject* packets transmitted by the encryption control protocol.
outTerminateRequest	The number of *Terminate-Request* packets transmitted by the encryption control protocol.
outTerminateAcknowledge	The number of *Terminate-Acknowledge* packets transmitted by the encryption control protocol.
outCodeReject	The number of *Code-Reject* packets transmitted by the encryption control protocol.
outResetRequests	The number of *Reset-Request* packets transmitted to reset the compression history.
outResetACKs	The number of *Reset-Acknowledge* packets transmitted to reset the compression history.
encodeSuccesses	The number of packets successfully encoded.
encodeFailures	The number of packets that failed to be encoded correctly.
encodeDiscards	The number of packets to be encoded that were discarded.
getSessKeyFailures	The number of times the PPP interface failed to retrieve a session key from the STAR module.
getMktFailures	The number of times the PPP interface failed to retrieve a master key from the STAR module.
starEventsWithLcpDown	The number of times the PPP interface received an event from the STAR module when the interface's LCP was not in the OPENED state.
CCP ILCCP OVER: *<interface>*	Information about the compression control protocol (CCP) or ILCCP and the physical interface over which ILCCP is running.
inOctets	The number of octets received by the compression protocol. This includes two octets per frame for the PPP compression header, the number of octets of compressed data received, and the number of octets in control protocol packets (CCP). For multilinks an extra six octets per frame are included for the multilink header.
inUserPkts	The number of packets received by the compression control protocol.
inConfigureRequest	The number of *Configure-Request* packets received by the compression control protocol.
inConfigureAcknowledge	The number of *Configure-Acknowledge* packets received by the compression control protocol.
inConfigureNAK	The number of *Configure-NAK* packets received by the compression control protocol.
inConfigureReject	The number of *Configure-Reject* packets received by the compression control protocol.
inTerminateRequest	The number of *Terminate-Request* packets received by the compression control protocol.

Table 3-10: Parameters displayed in the output of the SHOW PPP COUNT=LCP command. (Continued)

Parameter	Meaning
inTerminateAcknowledge	The number of *Terminate-Acknowledge* packets received by the compression control protocol.
inCodeReject	The number of *Code-Reject* packets received by the compression control protocol.
decodeSuccesses	The number of packets successfully decoded by the compression or encryption control protocol.
decodeFailures	The number of packets that failed to be decoded correctly by the compression or encryption control protocol.
decodeDiscards	The number of packets that were discarded by the compression or encryption control protocol.
inResetRequests	The number of *Reset-Request* packets received to reset the compression history.
inResetACKs	The number of *Reset-Acknowledge* packets received to reset the compression history.
encoEventsWithLcpDown	The number of times the PPP interface received an event from the ENCO module when the interface's LCP was not in the OPENED state.
outOctets	The number of octets transmitted by the compression protocol. This includes two octets per frame for the PPP compression header, the number of octets of compressed data transmitted, and the number of octets in control protocol packets (CCP). For multilinks an extra six octets per frame are included for the multilink header.
outUserPkts	The number of packets transmitted by the compression control protocol.
outConfigureRequest	The number of *Configure-Request* packets transmitted by the compression control protocol.
outConfigureAcknowledge	The number of *Configure-Acknowledge* packets transmitted by the compression control protocol.
outConfigureNAK	The number of *Configure-NAK* packets transmitted by the compression control protocol.
outConfigureReject	The number of *Configure-Reject* packets transmitted by the compression control protocol.
outTerminateRequest	The number of *Terminate-Request* packets transmitted by the compression control protocol.
outTerminateAcknowledge	The number of *Terminate-Acknowledge* packets transmitted by the compression control protocol.
outCodeReject	The number of *Code-Reject* packets transmitted by the compression control protocol.
encodeSuccesses	The number of packets successfully encoded.
encodeFailures	The number of packets that failed to be encoded correctly.
encodeDiscards	The number of packets to be encoded that were discarded.
outResetRequests	The number of *Reset-Request* packets transmitted to reset the compression history.
outResetACKs	The number of *Reset-Acknowledge* packets transmitted to reset the compression history.

Table 3-10: Parameters displayed in the output of the SHOW PPP COUNT=LCP command. (Continued)

Parameter	Meaning
LQM OVER: *<interface>*	Information about LQR and the physical interface over which LQR is running.
lqrFailures	The number of times the LQR timer has timed out.
loopbacksDetected	The number of times the link entered loopback mode.
inLQRs	The number of LQR packets received.
inPktLost	The number of inbound LQR packets lost.
inOctetLost	The number of inbound LQR octets lost.
outLQRs	The number of LQR packets transmitted.
outPktLost	The number of outbound LQR packets lost.
outOctetLost	The number of outbound LQR octets lost.
outLQRsLost	The number of outbound LQR packets lost.
outLQRsTransit	The number of outbound LQR packets in transit.
PAP OVER: *<interface>*	Information about PAP and the physical interface over which PAP is running.
inRequest	The number of PAP *Authenticate-Request* packets received.
inAck	The number of PAP *Authenticate-Acknowledgement* packets received.
inNak	The number of PAP *Authenticate-Negative-Acknowledgement* packets received.
outRequest	The number of PAP *Authenticate-Request* packets transmitted.
outAck	The number of PAP *Authenticate-Acknowledgement* packets transmitted.
outNak	The number of PAP *Authenticate-Negative-Acknowledgement* packets transmitted.
CHAP OVER: *<interface>*	Information about CHAP and the physical interface over which CHAP is running.
inChallenge	The number of CHAP *Challenge* packets received for.
inResponse	The number of CHAP *Response* packets received.
inSuccess	The number of CHAP *Success* packets received.
inFailure	The number of CHAP *Failure* packets received.
outChallenge	The number of CHAP *Challenge* packets transmitted.
outResponse	The number of CHAP *Response* packets transmitted.
outSuccess	The number of CHAP *Success* packets transmitted.
outFailure	The number of CHAP *Failure* packets transmitted.
LCP OVER: *<interface>*	Information about the LCP and the physical interface over which LCP is running.

Table 3-10: Parameters displayed in the output of the SHOW PPP COUNT=LCP command. (Continued)

Parameter	Meaning
inOctets	The number of octets received by the link control protocol. This includes the number of octets in control protocol packets (e.g. LCP, LQR, PAP, CHAP), plus the number of octets of data received. The number of octets of data will be equal to the number of inOctets recorded for compression or encryption if they are enabled. If they are not enabled the number of inOctets of data will be equal to the sum of the inOctets recorded for all the user protocols on this link. For multilinks an extra six octets per frame are included for the multilink header.
inUserPkts	The number of packets received for the LCP.
inConfigureRequest	The number of *Configure-Request* packets received for the LCP.
inConfigureAcknowledge	The number of *Configure-Acknowledge* packets received for the LCP.
inConfigureNAK	The number of *Configure-NAK* packets received for the LCP.
inConfigureReject	The number of *Configure-Reject* packets received for the LCP.
inTerminateRequest	The number of *Terminate-Request* packets received for the LCP.
inTerminateAcknowledge	The number of *Terminate-Acknowledge* packets received for the LCP.
inCodeReject	The number of *Code-Reject* packets received for the LCP.
inProtocolReject	The number of Protocol Reject packets received for the LCP.
inEchoRequest	The number of Echo Request packets received for the LCP.
inEchoReply	The number of Echo Reply packets received for the LCP.
inDiscardRequest	The number of Discard Request packets received for the LCP.
echoFailures	The number of times the ECHO timer has timed out.
outOctets	The number of octets transmitted by the LCP. This includes the number of octets in control protocol packets (e.g. LCP, LQR, PAP, CHAP), plus the number of octets of data transmitted. The number of octets of data will be equal to the number of outOctets recorded for compression or encryption if they are enabled. If they are not enabled the number of outOctets of data will be equal to the sum of the outOctets recorded for all the user protocols on this link. For multilinks an extra six octets per frame are included for the multilink header.
outUserPkts	The number of packets sent for the LCP.
outConfigureRequest	The number of *Configure-Request* packets sent for the LCP.
outConfigureAcknowledge	The number of *Configure-Acknowledge* packets sent for the LCP.
outConfigureNAK	The number of *Configure-NAK* packets sent for the LCP.
outConfigureReject	The number of *Configure-Reject* packets sent for the LCP.
outTerminateRequest	The number of *Terminate-Request* packets sent for the LCP.

Table 3-10: Parameters displayed in the output of the SHOW PPP COUNT=LCP command. (Continued)

Parameter	Meaning
outTerminateAcknowledge	The number of *Terminate-Acknowledge* packets sent for the LCP.
outCodeReject	The number of *Code-Reject* packets sent for the LCP.
outProtocolReject	The number of Protocol Reject packets sent for the LCP.
outEchoRequest	The number of Echo Request packets sent for the LCP.
outEchoReply	The number of Echo Reply packets sent for the LCP.
outDiscardRequest	The number of Discard Request packets sent for the LCP.
badEchoReplies	The number of *Echo Reply* packets received with a different ID than the original *Echo Request* packet.

Figure 3-18: Example output from the SHOW PPP COUNT=MULTILINK command.

```
Multilink Counters
  inWholeFragments            1538     outWholeFragments            1538
  inStartFragments               0     outStartFragments               0
  inMiddleFragments              0     outMiddleFragments              0
  inEndFragments                 0     outEndFragments                 0
  inNullFragments               54     outNullFragments               54
```

Table 3-11: Parameters displayed in the output of the SHOW PPP COUNT=MULTILINK command.

Parameter	Meaning
inWholeFragments	The number of multilink encapsulated fragments received that contain a whole packet.
inStartFragments	The number of multilink encapsulated fragments received that contain the start of a packet.
inMiddleFragments	The number of multilink encapsulated fragments received that contain part of a packet that is not the start or the end.
inEndFragments	The number of multilink encapsulated fragments received that contain the end of a packet.
inNullFragments	The number of NULL multilink encapsulated fragments that have been received.
outWholeFragments	The number of multilink encapsulated fragments transmitted that contain a whole packet.
outStartFragments	The number of multilink encapsulated fragments transmitted that contain the start of a packet.
outMiddleFragments	The number of multilink encapsulated fragments transmitted that contain part of a packet that is not the start or the end.
outEndFragments	The number of multilink encapsulated fragments transmitted that contain the end of a packet.
outNullFragments	The number of NULL multilink encapsulated fragments that have been transmitted.

Figure 3-19: Example output from the SHOW PPP COUNT=NCP command.

```
IPCP
  inOctets                   63611     outOctets                   91768
  inUserPkts                  2098     outUserPkts                  1538
  inConfigureRequest             1     outConfigureRequest             1
  inConfigureAcknowledge         1     outConfigureAcknowledge         1
  inConfigureNAK                 0     outConfigureNAK                 0
  inConfigureReject              0     outConfigureReject              0
  inTerminateRequest             0     outTerminateRequest             0
  inTerminateAcknowledge         0     outTerminateAcknowledge         0
  inCodeReject                   0     outCodeReject                   0
```

Table 3-12: Parameters displayed in the output of the SHOW PPP COUNT=NCP command.

Parameter	Meaning
inOctets	The number of octets received by the network protocol. This includes two octets per frame for the PPP protocol header, the number of octets of user data to be passed up to the user protocol, and the number of octets in control protocol packets (e.g. IPCP, ATCP).
inUserPkts	The number of packets received for the network control protocol.
inConfigureRequest	The number of Configure-Request packets received for the network control protocol.
inConfigureAcknowledge	The number of Configure-Acknowledge packets received for the network control protocol.
inConfigureNAK	The number of Configure-NAK packets received for the network control protocol.
inConfigureReject	The number of Configure-Reject packets received for the network control protocol.
inTerminateRequest	The number of Terminate-RequestTerminate-Acknowledge packets received for the network control protocol.
inTerminateAcknowledge	The number of Terminate-Acknowledge packets received for the network control protocol.
inCodeReject	The number of Code-Reject packets received for the network control protocol.
outOctets	The number of octets transmitted by the network protocol. This includes two octets per frame for the PPP protocol header, the number of octets of user data passed down from the user protocol, and the number of octets in control protocol packets (e.g. IPCP, ATCP).
outUserPkts	The number of packets sent for the network control protocol.
outConfigureRequest	The number of Configure-Request packets sent for the network control protocol.
outConfigureAcknowledge	The number of Configure-Acknowledge packets sent for the network control protocol.
outConfigureNAK	The number of Configure-NAK packets sent for the network control protocol.
outConfigureReject	The number of Configure-Reject packets sent for the network control protocol.

Table 3-12: Parameters displayed in the output of the SHOW PPP COUNT=NCP command. (Continued)

Parameter	Meaning
outTerminateRequest	The number of Terminate-Request packets sent for the network control protocol.
outTerminateAcknowledge	The number of Terminate-Acknowledge packets sent for the network control protocol.
outCodeReject	The number of Code-Reject packets sent for the network control protocol.

Table 3-13: Parameters displayed in the output of the SHOW PPP COUNT command for BAP and BACP.

Parameter	Meaning
BAP	Information about the operation of BAP.
inCallReq	The number of *Call-Request* packets received by the BAP protocol.
inCallResp	The number of *Call-Response* packets received by the BAP protocol.
inCallbackReq	The number of *Callback-Request* packets received by the BAP protocol.
inCallbackResp	The number of *Callback-Response* packets received by the BAP protocol.
inLinkDropQueryReq	The number of *Link-Drop-Query-Request* packets received by the BAP protocol.
inLinkDropQueryResp	The number of *Link-Drop-Query-Response* packets received by the BAP protocol.
inCallStatusInd	The number of *Call-Status-Indication* packets received by the BAP protocol.
inCallStatusResp	The number of *Call-Status-Response* packets received by the BAP protocol.
inErrors	The number of packets received by the BAP protocol which contained errors.
inDiscards	The number of packets received by the BAP protocol that were discarded.
outCallReq	The number of *Call-Request* packets transmitted by the BAP protocol.
outCallResp	The number of *Call-Response* packets transmitted by the BAP protocol.
outCallbackReq	The number of *Callback-Request* packets transmitted by the BAP protocol.
outCallbackResp	The number of *Callback-Response* packets transmitted by the BAP protocol.
outLinkDropQueryReq	The number of *Link-Drop-Query-Request* packets transmitted by the BAP protocol.
outLinkDropQueryResp	The number of *Link-Drop-Query-Response* packets transmitted by the BAP protocol.
outCallStatusInd	The number of *Call-Status-Indication* packets transmitted by the BAP protocol.

Table 3-13: Parameters displayed in the output of the SHOW PPP COUNT command for BAP and BACP. (Continued)

Parameter	Meaning
outCallStatusResp	The number of *Call-Status-Response* packets transmitted by the BAP protocol.
BACP	Information about the operation of BACP.
inOctets	The number of octets received by the BACP protocol.
inUserPkts	The number of packets received by the BACP protocol.
inConfigureRequest	The number of *Configure-Request* packets received by the BACP protocol.
inConfigureAcknowledge	The number of *Configure-Acknowledge* packets received by the BACP protocol.
inConfigureNAK	The number of *Configure-NAK* packets received by the BACP protocol.
inConfigureReject	The number of *Configure-Reject* packets received by the BACP protocol.
inTerminateRequest	The number of *Terminate-Request* packets received by the BACP protocol.
inTerminateAcknowledge	The number of *Terminate-Acknowledge* packets received by the BACP protocol.
inCodeReject	The number of *Code-Reject* packets received by the BACP protocol.
outOctets	The number of octets transmitted by the BACP protocol.
outUserPkts	The number of packets transmitted by the BACP protocol.
outConfigureRequest	The number of *Configure-Request* packets transmitted by the BACP protocol.
outConfigureAcknowledge	The number of *Configure-Acknowledge* packets transmitted by the BACP protocol.
outConfigureNAK	The number of *Configure-NAK* packets transmitted by the BACP protocol.
outConfigureReject	The number of *Configure-Reject* packets transmitted by the BACP protocol.
outTerminateRequest	The number of *Terminate-Request* packets transmitted by the BACP protocol.
outTerminateAcknowledge	The number of *Terminate-Acknowledge* packets transmitted by the BACP protocol.
outCodeReject	The number of *Code-Reject* packets transmitted by the BACP protocol.

Examples

To display the interface counters for PPP interface 1, use the command:

```
SHOW PPP=1 COUNT=INTERFACE
```

See Also

SHOW PPP
SHOW PPP CONFIG
SHOW PPP IDLETIMER
SHOW PPP MULTILINK

SHOW PPP DEBUG

Syntax `SHOW PPP[=`*`ppp-interface`*`] DEBUG`

where:

- *ppp-interface* is the PPP interface number.

Description This command displays the debugging options that are currently enabled for the specified or all PPP interfaces (Figure 3-20 on page 3-83, Table 3-14 on page 3-83).

Figure 3-20: Example output from the SHOW PPP DEBUG command.

```
Interface        Enabled Debug Modes
-----------------------------------------------------------
ppp0             AUTH, LCP, PKT, UTILISATION
-----------------------------------------------------------
```

Table 3-14: Parameters displayed in the output of the SHOW PPP DEBUG command.

Parameter	Meaning
Interface	The interface name.
Enabled Debug Modes	The list of currently enabled debug modes for the interface; one or more of "AUTH", "BAPPKT", "BAPSTATE", "CALLBACK", "DEMAND", "ENCO", "LCP", "NCP", "PKT" or "UTILISATION".

Examples To display the debugging options set for all PPP interfaces, use the command:

```
SHOW PPP DEBUG
```

See Also DISABLE PPP DEBUG
ENABLE PPP DEBUG

SHOW PPP IDLETIMER

Syntax `SHOW PPP[=`*`ppp-interface`*`] IDLETIMER`

where:

- *ppp-interface* is the PPP interface number.

Description This command displays the configured and current values of the PPP idle timer for the specified or all PPP interfaces (Figure 3-21 on page 3-84, Table 3-15 on page 3-84).

Figure 3-21: Example output from the SHOW PPP IDLETIMER command.

```
Interface
  Configured Idle Time       Idle Timer Value
-------------------------------------------
ppp0
                    60               EXPIRED
-------------------------------------------
```

Table 3-15: Parameters displayed in the output of the SHOW PPP IDLETIMER command.

Parameter	Meaning
ppp0	The interface name.
Configured Idle Time	The configured value, in seconds, of the idle timer for the interface.
Idle Timer Value	The current value, in seconds, of the idle timer for the interface, or "EXPIRED" if the timer has expired.

Examples To display the idle timers for all PPP interfaces, use the command:

```
SHOW PPP IDLETIMER
```

See Also SHOW PPP
SHOW PPP CONFIG
SHOW PPP COUNT
SHOW PPP MULTILINK

SHOW PPP MULTILINK

Syntax `SHOW PPP[=`*`ppp-interface`*`] MULTILINK`

where:

- *ppp-interface* is the PPP interface number.

Description This command displays information about the multilink bundle for the specified or all PPP interfaces (Figure 3-22 on page 3-85, Table 3-16 on page 3-85).

Figure 3-22: Example output from the SHOW PPP MULTILINK command.

```
Interface
  Parameter                                                              Value
-------------------------------------------------------------------------------
ppp0
  Multilink Enabled                                                        Yes
  Fragmentation Enabled                                                     No
  Acceptable fragmentation overhead for VF scheme (%)                        5
  Minimum packet size for fragmentation using VF scheme (bytes)            120
  Null fragment timer (seconds)                                              3
  Number of links in bundle                                                  4
  Total bandwidth of bundle (bps)                                       256000
  Number of packets fragmented using VF scheme                               0
  Number of packets fragmented using FF scheme                               0
  Number of packets not fragmented                                         971
  Next output sequence number                                              972
  Minimum sequence number received on bundle                               863
  Next expected sequence number                                            866
  Length of receive queue                                                    0
  Discards from receive queue                                                0
-------------------------------------------------------------------------------
```

Table 3-16: Parameters displayed in the output of the SHOW PPP MULTILINK command.

Parameter	Meaning
ppp0	The interface name.
Multilink Enabled	Whether or multilink is enabled on this PPP interface; one of "Yes" or "No".
Fragmentation Enabled	Whether or fragmentation is enabled on this PPP interface; one of "Yes" or "No".
Acceptable fragmentation overhead for VF scheme (%)	The maximum acceptable overhead for fragmentation using the variable fragmentation scheme, as a percentage of packet size.
Minimum packet size for fragmentation using VF scheme (bytes)	The minimum size packet that may be fragmented using the variable fragmentation scheme.
Null fragment timer (seconds)	The time, in seconds, the link must be idle before a null fragment is transmitted.
Number of links in bundle	The number of links in the multilink bundle.
Total bandwidth of bundle (bps)	The total bandwidth, in bits per second, of the multilink bundle.

Table 3-16: Parameters displayed in the output of the SHOW PPP MULTILINK command. (Continued)

Parameter	Meaning
Number of packets fragmented using VF scheme	The number of packets that have been fragmented using the variable fragmentation scheme.
Number of packets fragmented using FF scheme	The number of packets that have been fragmented using the fixed fragmentation scheme.
Number of packets not fragmented	The number of packets that have not been fragmented.
Next output sequence number	The sequence number to use in the next transmission over the multilink bundle.
Minimum sequence number received on bundle	The lowest sequence number received via the multilink bundle.
Next expected sequence number	The next sequence number expected via the multilink bundle.
Length of receive queue	The current length of the receive queue.
Discards from receive queue	The number of packets discarded from the receive queue due to lost packets causing sequence number synchronisation to be lost.

Examples To display multilink information for all PPP interfaces, use the command:

```
SHOW PPP MULTILINK
```

See Also SHOW PPP
SHOW PPP CONFIG
SHOW PPP COUNT
SHOW PPP IDLETIMER

SHOW PPP NAMESERVER

Syntax `SHOW PPP NAMESERVER`

Description This command displays information about the currently configured global DNS and WINS servers (Figure 3-23 on page 3-86, Table 3-17 on page 3-87).

Figure 3-23: Example output from the SHOW PPP NAMESERVER command.

```
Name Server                      Address
-------------------------------------------------
Primary DNS ..................... 192.168.2.3
Secondary DNS ................... 192.168.5.1
Primary WinS .................... 192.168.5.5
Secondary WinS .................. Not Set
-------------------------------------------------
```

Table 3-17: Parameters displayed in the output of the SHOW PPP NAMESERVER command.

Parameter	Meaning
Primary DNS Address	The IP address of the primary DNS server, passed to a peer in response to an IPCP primary DNS request.
Secondary DNS Address	The IP address of the secondary DNS server, passed to a peer in response to an IPCP secondary DNS request.
Primary WinS Address	The IP address of the primary WINS server, passed to a peer in response to an IPCP primary WINS server request.
Secondary WinS Address	The IP address of the secondary WINS server, passed to a peer in response to an IPCP secondary WINS server request.

Examples To display the currently configure DNS and WINS servers, use the command:

```
SHOW PPP NAMESERVER
```

See Also SET PPP
SHOW PPP

SHOW PPP TEMPLATE

Syntax `SHOW PPP TEMPLATE[=`*`template`*`] [DEBUG]`

where:

- *template* is a number in the range 0 to 31.

Description This command displays information about PPP templates.

The TEMPLATE parameter specifies the number of the template to display. If a template is not specified, information about all templates, including the default template, is displayed. If a template is specified, information about the specified template is displayed (Figure 3-24 on page 3-88, Table 3-18 on page 3-88). If no templates have been defined, the default template is displayed.

If DEBUG is specified, the debugging modes enabled for the template or all templates are displayed (Figure 3-25 on page 3-90, Table 3-19 on page 3-90).

Figure 3-24: Example output from the SHOW PPP TEMPLATE command.

```
Template - Description
  Parameter                                          Value
-------------------------------------------------------------------------------
pppt0 - Template for ACC calls from Head Office
  Maximum links                                        4
  Bandwidth Allocation Protocol                       ON
  Bandwidth Allocation Call Mode                    CALL
  Multilink fragmentation                            OFF
  Acceptable Fragment Overhead (%)                     5
  Null Fragment Timer (seconds)                        3
  Idle Timer (seconds)                               OFF
  Compression                                         ON
  Compression Algorithm                           STACLZS
  Compression Checkmode                               LCB
  Encryption                                         OFF
  Username                                       NOT SET
  Password                                       NOT SET
  Login Servers                  USER,RADIUS,TACACS
  Request IP Address                                  NO
Link
  Authentication                                    NONE
  Callback Mode                                      OFF
  Callback Operation                                USER
  Callback Number                                      -
  Callback Delay (seconds)                             5
  Echo Timer (seconds)                                10
  LQR Timer (seconds)                                 60
  Magic Number                                        ON
  Restart Timer (seconds)                              3
Debug
  Maximum packet bytes to display                     32
-------------------------------------------------------------------------------
```

Table 3-18: Parameters displayed in the output of the SHOW PPP TEMPLATE command.

Parameter	Meaning
pppT<*template*> - <*description*>	The number and description of the template.
Maximum links	The maximum number of links allowed in a multilink bundle created with this template.
Bandwidth Allocation Protocol	Whether or not the Bandwidth Allocation Protocol is enabled; one of "ON" or "OFF".
Bandwidth Allocation Call Mode	The call mode for the Bandwidth Allocation Protocol, if the Bandwidth Allocation Protocol is enabled; one of "CALL" or "CALLBACK".
Multilink fragmentation	Whether or not multilink packets may be fragmented; one of "ON" or "OFF".
Acceptable Fragment Overhead(%)	The maximum amount of overhead allowed to be added to each packet due to variable fragmentation. If this level is exceeded when fragmentation of a packet is done using the variable fragmentation scheme, then the fixed fragmentation scheme is used instead.
Null Fragment Timer	The time, in seconds, that the link must be idle for before a Null fragment is sent on a link in a multilink bundle.

Table 3-18: Parameters displayed in the output of the SHOW PPP TEMPLATE command. (Continued)

Parameter	Meaning
Idle Timer (seconds)	The length of time, in seconds, a link must be idle before it is disconnected, or "OFF" if the idle timer is disabled.
Compression	Whether or not compression is enabled; one of "ON" or "OFF".
Compression Algorithm	The compression algorithm to use for compressing packets; one of "PREDICTOR" or "STACLZS".
Compression Checkmode	The check mode used by the compression algorithm to determine when a decompression history becomes unsynchronised; one of "SEQUENCE", "LCB", "CRC16" or "CRCCCITT".
Encryption	Whether or not encryption is enabled; one of "ON" or "OFF".
Username	The username used by the PPP interface for both PAP and CHAP authentication, or "NOT SET" if a username has not been set.
Password	Whether or not a password has been set for the entire PPP interface; one of "SET" or "NOT SET".
Login Servers	The authentication servers to use; one or more of "USER", "RADIUS", "TACACS", "TACACSPLUS", or "NOT SET" if a login server has not been set.
Request IP Address	Whether or not an IP address will be requested from the peer during IPCP negotiation; one of "ON" or "OFF".
Authentication	The authentication protocol in use; one of "NONE", "PAP", "CHAP" or "EITHER".
Callback Mode	Whether the link will request callback, accept callback or do neither; one of "REQUEST", "ACCEPT" or "OFF".
Callback Operation	The callback operation included in callback requests; one of "USERAUTH" or "E164NUMBER".
Callback Number	The callback number to include in callback requests when the callback operation is E164NUMBER.
Callback Delay (seconds)	The delay, in seconds, between deactivating a call for callback and making the call back to the peer.
Echo Timer (seconds)	The interval, in seconds, between transmissions of LCP *Echo Request* messages.
LQR Timer (seconds)	The time in seconds between LQR packets transmitted over the physical interface.
Magic Number	Whether or not the magic number option is enabled; one of "ON" or "OFF".
Restart Timer	The time in seconds between configure requests for the physical interface.
Maximum packet bytes to display	The maximum number of bytes of each PPP packet displayed by the PACKET debugging option.

Figure 3-25: Example output from the SHOW PPP TEMPLATE DEBUG command.

```
Template      Call                      Enabled Debug Modes
-------------------------------------------------------------------
pppT0                                   PKT,LCP,NCP
-------------------------------------------------------------------
```

Table 3-19: Parameters displayed in the output of the SHOW PPP TEMPLATE DEBUG command.

Parameter	Meaning
Template	The name of a PPP template.
Call	The lower layer call using this template, if any.
Enabled Debug Modes	The debugging modes enabled for the template (and call); one or more of "AUTH", "BAPPKT", "BAPSTATE", "CALLBACK", "DEMAND", "ENCO", "LCP", "NCP", "PKT" or "UTILISATION".

Examples To display the configuration for all templates, use the command:

```
SHOW PPP TEMPLATE
```

To display the configuration for template 1, use the command:

```
SHOW PPP TEMPLATE=1
```

To display the debugging modes enabled for template 3, use the command:

```
SHOW PPP TEMPLATE=3 DEBUG
```

See Also CREATE PPP TEMPLATE
DESTROY PPP TEMPLATE
DISABLE PPP TEMPLATE DEBUG
ENABLE PPP TEMPLATE DEBUG
SET PPP TEMPLATE

SHOW PPP TXSTATUS

Syntax `SHOW PPP[=`*`ppp-interface`*`] TXSTATUS`

where:

- *template* is a number in the range 0 to 31.

Description This command displays information about the status of a PPP transmission queue for the specified interface of all interfaces (Figure 3-26 on page 3-91, Table 3-20 on page 3-91).

Figure 3-26: Example output from the SHOW PPP TXSTATUS command.

```
Interface
  Parameter                                          Value
-------------------------------------------------------
ppp0
  Interface transmission queue length .......... 0

syn0
  Packets started transmission ................. 198
  Packets being transmitted .................... 0
  Packets lost during transmission ............. 3
  Packets finished transmission ................ 195
  Packets discarded in pipe .................... 0
  Link transmission queue length ............... 0
  Driver bandwidth (bps) ....................... 48000
  Driver transmission delay (ms) ............... 0
  Driver transmission status ................... Ready
-------------------------------------------------------
```

Table 3-20: Parameters displayed in the output of the SHOW PPP TXSTATUS command.

Parameter	Meaning
ppp*<n>*	The name of a PPP interface.
Interface transmission queue length	The length of the output queue for this PPP interface.
<physical-interface>	The name of a physical interface or channel forming part of this PPP interface.
Packets started transmission	The total number of packets that higher-layer protocols requested be transmitted to a non-unicast address, including those that were discarded or not sent.
Packets being transmitted	The number of packets currently being transmitted on this physical interface or channel.
Packets lost during transmission	The number of packets lost during transmission on this physical interface or channel.
Packets finished transmission	The number of packets that have been transmitted and acknowledged on this physical interface or channel.
Packets discarded in pipe	The number of packets that were discarded on this physical interface or channel.
Link transmission queue length	The length of the output queue for this physical interface or channel.
Driver bandwidth (bps)	The bandwidth of the layer 1 device driver for this physical interface or channel.
Driver transmission delay (ms)	The delay, in milliseconds, in the layer 1 device driver for this physical interface or channel.
Driver transmission status	The status of the layer 1 device driver for this physical interface or channel; one of "busy" or "ready".

Examples To display the status of the PPP transmission queue for interface ppp0, use the command:

```
SHOW PPP=0 TXSTATUS
```

See Also SET PPP
SHOW PPP